UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA - v. - JOSHUA ADAM SCHULTE, Defendant.	S3 17 Cr. 548 (JMF)

THE GOVERNMENT'S MEMORANDUM OF LAW IN OPPOSITION TO THE DEFENDANT'S *PRO SE* MOTIONS FOR A JUDGMENT OF ACQUITTAL OR NEW TRIAL

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York

David W. Denton, Jr.
Michael D. Lockard
Assistant United States Attorneys
Of Counsel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND REGULATIONS

OTHER AUTHORITIES

RULES

PRELIMINARY STATEMENT

The Government respectfully submits this memorandum of law in opposition to defendant Joshua Adam Schulte's *pro se* motions for acquittal pursuant to Federal Rule of Criminal Procedure 29 and a new trial pursuant to Rule 33. (D.E. 992) (the "Motion"). Following a month-long trial, Schulte was found guilty of four counts of espionage in violation of 18 U.S.C. §§ 793(b) and (e), four counts of computer hacking in violation of 18 U.S.C. § 1030(a), and one count of obstructing justice in violation of 18 U.S.C. § 1503. As detailed below, the evidence of Schulte's guilt was overwhelming, and readily sufficient to sustain the jury's verdict.

Schulte's motion for a new trial based on the contention that he was unfairly denied access to complete forensic images of the entire CIA DevLAN network, including overseas network components and every connected device, is meritless. Prior to trial, the Court denied Schulte's repeated requests for complete access to enormous volumes of classified, irrelevant, and unhelpful information, and Schulte's motion pursuant to Rule 33 consists of a rehash of previously rejected arguments, new theories that were never previously presented to the Court, and mischaracterizations of the evidence and procedural history. He fails to show any error in the Court's rulings, much less manifest injustice requiring a new trial.

BACKGROUND

I. The Indictment

On June 8, 2020, Schulte was charged in a superseding indictment, S3 17 Cr. 548 (JMF) (the "Indictment"), with offenses arising out of his April 2016 theft of the CIA's cyber tool arsenal and his transmittal of that library of classified information to WikiLeaks.org ("WikiLeaks"); his obstruction of a resulting grand jury investigation that commenced when WikiLeaks began serially publishing portions of the stolen information; and his disclosure of, and attempts to disclose,

additional classified, national defense information from prison using pseudonymous email and social media accounts Schulte created using a contraband prison cellphone.

Specifically, the Indictment charged Schulte with (1) two counts of illegally gathering and transmitting materials relating to the national defense, 18 U.S.C. § 793(b) and (e), in connection with his April 2016 theft of classified information from the CIA and transmittal to WikiLeaks (Counts One and Two); (2) two counts of illegally transmitting and attempting to transmit materials relating to the national defense, 18 U.S.C. § 793(e), in connection with his 2018 disclosure and attempted disclosure of classified information after being charged in this case from the Metropolitan Correctional Center (the "MCC") (Counts Three and Four); (3) four counts of unauthorized access to computers and transmission of harmful computer commands, 18 U.S.C. § 1030(a)(1), (a)(2), and (a)(5), in connection with Schulte's April 2016 unauthorized access to and manipulation of CIA computer systems and theft of classified information (Counts Five through Eight); and (4) one count of obstructing justice, 18 U.S.C. § 1503, in connection with false statements Schulte made to the FBI during its investigation (Count Nine).[1]

II. Trial

Trial commenced on June 13, 2022, and concluded on July 13, 2022, when the jury returned a verdict of guilty on all counts. Schulte represented himself at trial.

The Government called nine witnesses: two FBI special agents who participated in the investigation that led to the charges in the Indictment; three of Schulte's former CIA colleagues, including one of his supervisors and two developer colleagues; the former Deputy Director of the

[1] Schulte was found guilty at a prior trial of one count of contempt of court, 18 U.S.C. § 503, in connection with his 2018 disclosure of discovery materials subject to a protective order to a reporter while Schulte was at the MCC; and one count of making false statements, 18 U.S.C. § 1001 in connection with lies Schulte told the FBI in March 2017.

CIA directorate where Schulte worked; two expert witnesses on computer networks and forensics; and a former MCC inmate who provided Schulte access to contraband cellphones.

The Government also offered hundreds of exhibits, including records from Schulte's employment at the CIA; computer forensics from CIA computers and network infrastructure; documents from the WikiLeaks leak; documents and electronic evidence recovered from a search of Schulte's home and searches of his cloud accounts; computer forensics from Schulte's home computer; documents recovered from a search of Schulte's MCC cell; records from contraband cellphones Schulte used at the MCC; and evidence recovered from searches of pseudonymous email and social media accounts Schulte created with the contraband cellphones. At the conclusion of the Government's case, Schulte called three witnesses: a former paralegal for Schulte's defense team and two former CIA colleagues. Schulte did not testify.

A. The Government's Case

1. Schulte's Work As a Developer At the CIA's CCI

In 2015 and 2016, Schulte was employed by the CIA as a developer in the Center for Cyber Intelligence ("CCI"), which conducts offensive cyber operations, that is, cyber espionage relating to foreign governments or terrorist organizations. (Tr. 449-50, 1361, 1661). CCI conducted its work in an undisclosed office in the Washington, D.C. metropolitan area, protected by fencing, security guards, and other access controls. (Tr. 462-63).

Schulte worked in the Applied Engineering Division ("AED"), which developed cyber tools for that mission. (GX89; Tr. 450, 466). AED was part of CCI's Engineering and Development Group ("EDG"). (GX89; Tr. 449-51). Until approximately March 2016 Schulte was assigned to the Operations Support Branch ("OSB") (Tr. 1359-60, 1620). OSB was particularly focused on counterterrorism, developing cyber tools designed to gain access to computer networks and gather intelligence information. (Tr. 466, 1360-61, 1426). OSB's tools were used in, among other thing,

human-enabled operations or asset-enabled operations—that is, cyber operations that involved a person with access to the computer network being targeted by the cyber tool. (Tr. 1360, 1620).

OSB was located in one of the vaults, or Sensitive Compartmented Information Facilities ("SCIFs") at CCI. (Tr. 463, 1625). Developers in AED used a particular closed, classified, computer network, called DevLAN, to develop cyber tools for the CIA. (Tr. 476-77, 568-70, 1362-63, 1620-21). AED's work developing cyber tools and the tools themselves were generally classified. (Tr. 467-68, 1367, 1369, 1621-23). Employees required a Top Secret security clearance (Tr. 454), and Schulte signed a Secrecy Agreement and a Sensitive Compartmented Information Nondisclosure Agreement with the CIA to permit him access to the classified information he would work with as a developer with AED. (GX405 at 9-10 & 11-12; *see also* GX405 at 14-24).

In addition to being a developer, Schulte was also, for a time, one of the administrators of the suite of development programs that OSB and other AED branches used to develop cyber tools. The tool suite, developed by Atlassian, included a Wiki platform for collaborative development called Confluence (Tr. 471-72, 1363, 1621); and a repository for source code (human-readable computer programming language) for AED's cyber tools called Stash. (Tr. 471, 1374, 1621). The Atlassian suite also included Bamboo, a continuous integration tool, and Jira, an issue tracking tool. (Tr. 620-21, 1368, 1378-79, 1474-75). The DevLAN network was administered by the Infrastructure Support Branch ("ISB"), which was part of a separate division from AED. (Tr. 522, 524, 1368, 1409). The administrators for the Atlassian tool suite initially were developers in OSB (Tr. 479, 1369-71), intended as a temporary circumstance until ISB assumed administrative responsibilities. (*See, e.g.*, Tr. 1370; GX1023, 1024). Administration of the Atlassian tool suite was transferred to ISB in April 2016—a transfer precipitated, as described more fully below, by Schulte's abuse of his Atlassian administrator privileges. The Atlassian administrators performed

configuration and maintenance functions for the Atlassian programs, and occasionally ensured the permissions—access settings that allowed developers to access projects for which they needed access, and which prevented access to projects for which they did not—were appropriately set according to the developers' need-to-know. (Tr. 1371; *see also* 1403, 1621).

2. April 14, 2016: Schulte Abuses His Atlassian Administrator Privileges

In late 2015 and early 2016, personnel conflicts within OSB led to Schulte and another developer being reassigned from OSB to other branches. Schulte and another OSB developer named Amol made complaints about each other to their managers and to CIA's security group. (*See, e.g.*, GX1020, GX1038; Tr. 1385-90, 1634-35).[2] Schulte filed an action in local court for a protective order against Amol, which was initially granted and later dismissed. (Tr. 484, 489-90, 1391; GX1041). To ameliorate the effects of this conflict and to comply with the terms of the protective order, Schulte and Amol were assigned to different desks within OSB to physically separate them. (GX1042; Tr. 483-86, 1392). At the end of March 2016, Schulte and Amol each was assigned to different branches: Schulte was reassigned to the Remote Development Branch ("RDB") and Amol to a branch known as MDB. (GX1046; Tr. 486-90, 1392).

Sean, the supervisor of OSB, and Jeremy Weber and Frank Stedman, two senior developers within OSB, discussed which of Schulte's projects would stay within OSB and which projects Schulte would take to RDB. (Tr. 1392-93, 1637-39). Schulte and Anthony Leonis, then-supervisor of RDB and also acting deputy chief and acting chief of AED, had a similar discussion. (Tr. 492). Schulte would continue with projects named "Shattered Assurance" and "Nader," while his other OSB projects would remain with that branch. (Tr. 492, 1393-94, 1638-39).

---

[2] Schulte's complaint against Amol included false allegations. (*See, e.g.*, Tr. 1387-91, 1635-37).

While Schulte was in OSB, he was one of a handful of administrators of a project known as "OSB Libraries," a vetted collection of cyber tool components intended to be used for rapid development and available to all of the AED development branches. (Tr. 493, 1394-95, 1638). The role of a project administrator was distinct from the system administrator and Atlassian administrator roles described above, *supra* 4-5. Development projects were stored in Stash, one of the Atlassian programs, and project administrators had the ability to set access privileges to the project for other users; that is, the project administrator could give another developer read-only access to a project, read/write access, or no access. (Tr. 1395). Any developer could submit code for inclusion in OSB Libraries, after which the code would undergo a peer review process, a final review by one of the OSB Libraries administrators, and then be "merged," or saved, to the OSB Libraries by one of the project administrators. (Tr. 1395).

When Schulte moved from OSB to RDB, he was no longer an administrator for the OSB Libraries, though he continued to have access to the library and the ability to submit code for review. (GX1207-53, GX1207-97, GX1703-1 at 9, GX1704-1 at 1; Tr. 1395, 1368-39). On Thursday, April 14, 2016—shortly after his move to RDB—however, Schulte confronted Mr. Weber (another OSB Libraries administrator) about Schulte's loss of administrator privileges for the OSB Libraries project. (GX1062 at 8; Tr. 1396). Schulte then spoke to Sean, then-supervisor of OSB, and when he returned, Schulte told Mr. Weber that Sean had approved Schulte being an administrator for OSB Libraries. (GX1062 at 8; Tr. 1396). Mr. Weber told Schulte that he (Mr. Weber) would discuss it with Sean, and Schulte responded, "[I] will eventually get access back to the libraries and that access should just be enabled now." (GX1062 at 8). Sean instructed Mr. Weber, however, not to change Schulte's OSB Libraries status. (Tr. 1397).

After speaking with Sean himself, Mr. Weber sent an email to Schulte, copying Mr. Leonis, Sean, Mr. Stedman, and another OSB developer, reiterating that Mr. Weber and Mr. Stedman would continue as the administrators for OSB Libraries, but Schulte would be able to contribute to the libraries. (GX1061 at 5; Tr. 495, 1398). Schulte replied to the email at 3:39 p.m., claiming that OSB Libraries had originally been Schulte's idea and asking to continue "my active role" with the libraries, *i.e.*, as an administrator. (GX1061 at 4). Mr. Leonis responded at 3:59 p.m., instructing Mr. Weber, Mr. Stedman, Schulte, and other developers to meet with a developer named JoJo who would be responsible for making OSB Libraries an AED-level resource. (GX1061 at 3-4). Mr. Leonis did not tell Schulte that he (Schulte) could resume his administrator role and did not intend for Schulte to be an administrator. (Tr. 497).

Minutes later, Schulte used his Atlassian administrator privileges to restore his administrator status for the OSB Libraries project in Stash. (GX1207-65, GX1207-97, GX1703-1 at 9, GX1704-1 at 1; *see also* Tr. 499, 1401, 1402-03). Before leaving the CCI offices that day, Mr. Weber checked the OSB Libraries permission settings and saw that Schulte had changed his permissions after the email exchange described above. (Tr. 1400). Mr. Weber perceived Schulte's abuse of his Atlassian administrator privileges as a security issue and promptly informed his supervisors, Sean and Mr. Leonis. (GX1602 at 10; Tr. 1401-02).

On Friday, April 15, 2016, Mr. Leonis discussed Schulte's abuse of his Atlassian administrator privileges with Mr. Weber; Sean; CIA security; human resources; Mike, who was then the deputy chief of the Engineering and Development Group ("EDG"), the group that oversaw AED; and Karen, then-chief of EDG. (GX1062 at 1-9; Tr. 500-12, 520-23). The claim that Schulte had abused his Atlassian administrator privileges was a "heavy accusation," and Mr. Leonis sought to carefully and quickly assess the situation. (Tr. 500, 503). The events set off alarm bells within

AED and EDG management. Schulte's willingness to disregard his supervisors' decisions about his access levels, his misuse of one set of administrator privileges to restore another set of privileges that had been revoked, and the enormous sensitivity of the data stored on DevLAN raised a serious question "whether Joshua should be permitted continued access [to] EDG's code bases in the future." (GX1062 at 3; Tr. 518-21; *see also* Tr. 1403). As a result of these discussions, Mike instructed Mr. Leonis that all AED developers would be removed as Atlassian administrators and that responsibility would be transferred immediately to ISB. (Tr. 522-23).

3. April 15, 2016: Schulte Begins Testing His Access to Altabackup and the OSB Server

While the leaders of EDG and AED were investigating and developing a response to Schulte's abuse of his Atlassian administrator privileges, Schulte started testing security on DevLAN, particularly his access to OSB's server and to the Atlassian backups.

Though ISB had system administrator responsibility for DevLAN as a whole, OSB had a dedicated server that was administered by OSB developers. In 2015 and early 2016, Schulte and Mr. Weber were the primary administrators for the OSB server.[3] (Tr. 1375-76). The server was used by OSB developers to create "virtual machines," that is, software simulations of physical computers that mimic the operations and functionality of computer systems. (Tr. 1376-77). OSB developers used virtual machines ("VMs") for cyber tool development purposes: a test VM could be created to mimicked a target network, and a cyber tool could be tested in that environment for development purposes. (Tr. 1377-78). The OSB server also ran the Confluence virtual server for

[3] The OSB server was an ESXi server, which is an operating system designed to run multiple virtual machines. (Tr. 742).

AED, a result of the fact that OSB's ESXi server was, at that time, new and powerful enough to run Confluence as a virtualized server. (Tr. 1376).

Backup copies of the Confluence virtual server and the Stash server[4] were saved to a directory on DevLAN called "Altabackup," created and maintained by ISB for that purpose. (Tr. 1382; *see also* GX1207-36). Schulte and Mr. Weber, the two Atlassian administrators in late 2015 and early 2016, were responsible for the backups, and when the backup storage location was moved from a local directory to Altabackup, Schulte modified the program that automatically created the backups to save them in the new location. (Tr. 1382-83). The Altabackup directory was accessed by "mounting" it, that is, creating a network link between the folder and the system accessing it. (Tr. 766, 1383-84). The Confluence virtual server running on the OSB ESXi server had a mount point to the Altabackup directory so that the Confluence backups could copy there, as did the Stash server. (Tr. 814-16, 1384). Only Atlassian administrators had authority to access the Altabackup directory. (Tr. 1410-11).

On Friday, April 15, 2016, Schulte had not yet been informed that his abuse of his Atlassian administrator privileges to restore his OSB Libraries administrator status had been discovered. As an Atlassian administrator, however, Schulte would have been aware that his actions could easily be uncovered and that his administrator status was in jeopardy. First, at approximately 2:43 p.m., Schulte began conducting internet research on using his Atlassian administrator privileges to view restricted Confluence pages. (GX1704-1 at 32, GX3501-1; Tr. 778). At that time, OSB maintained a Confluence page with information on accessing OSB VMs and infrastructure. (GX1202-5). Second, at approximately 3:36 p.m., Schulte logged in to the OSB server as a regular user, through

[4] The Stash server was an ISB server. (Tr. 1373-74).

his vSphere application from his workstation. (GX1703-1 at 11, GX1209-09; Tr. 811-12). Schulte also logged in to the OSB server as "root," or administrator, at approximately 3:39 p.m. (GX1703-1 at 15-20, GX1209-13, GX1203-18; Tr. 816-20). Administering the OSB server was an OSB responsibility, and Schulte was no longer authorized to exercise administrator functions on the server when he was assigned to RDB. (Tr. 1601). Schulte logged into the OSB server using an SSH key login, an authentication methodology that relies on public and private key pairs. (Tr. 752-53, 817-18). Schulte never closed this OSB administrator session. (Tr. 816, 843-44).

Finally, at approximately 3:47 p.m., Schulte attempted to create a mount point to the Altabackup directory from his user session on the OSB server. (GX1703-1 at 12, GX1202-7; Tr. 812-14). Schulte's attempt failed because he lacked the necessary network permissions to mount the Altabackup directory using his regular DevLAN user account. (GX1703-1 at 13, GX1202-8; Tr. 814-16, 1087).

4. April 16, 2016: EDG Removes Schulte's Atlassian Administrator Privileges and OSB Server Administrator Privileges

Mike's instructions to transfer Atlassian administrator responsibilities to ISB were carried out the following day, Saturday, April 16, 2016. (Tr. 523-24, 1406-07). Mr. Weber and two ISB officers went to the CCI offices that morning and first created a "snapshot" of the Confluence virtual server and the Bamboo virtual server. (Tr. 1407-08). A "snapshot" is a file that preserves the state of a virtual machine at a particular point in time and allows a system administrator to revert back to that snapshot if necessary for system administration purposes—for example, if a system update creates problems, reverting to a snapshot taken prior to the update restores the virtual machine to prior state. (Tr. 742-43, 746, 1377-78). The Confluence snapshot was saved on the OSB server as "bkup 4-16-2016." (GX1703-1 at 22, GX1207-92; Tr. 831-33).

After the snapshot was taken, ISB removed Atlassian administrator privileges from the OSB developers. Prior to April 16, 2016, there were seven authorized SSH keys on the Confluence virtual server—the public keys from SSH key pairs that were authorized to log in to the Confluence virtual server as an administrator—including Schulte's. On April 16, 2016, all seven SSH keys were deleted and one new SSH key was added. (GX1703-1 at 23-24, GX1207-7, GX1207-18; Tr. 833). ISB also changed the username/password administrator login to the Confluence virtual server on (GX1703-1 at 25, GX 1207-11, GX1207-21; Tr. 834) and removed Schulte and other AED developers from the administrator groups for the Atlassian products. (GX1704-1 at 2-3, GX1207-95, GX1207-96, GX1207-98, GX1207-99). These changes eliminated Schulte's ability to log in to the Confluence virtual server as an administrator, and removed his ability to access the Altabackup directory from the Confluence virtual server.

Mr. Weber also changed the username/password login for OSB's ESXi server. (GX1703-1 at 26-27, GX1209-12, GX1209-13, GX1209-15; Tr. 834-36, 1409). The SSH key authorizations for the OSB root account were not changed. Because of the particular version of the Linux operating system running on the OSB server, the location of the SSH keys was different than it would be in the normal case. (Tr. 838).

At the conclusion of ISB's changes to the DevLAN system, Mr. Weber tested the changes by attempting to log in to the Atlassian suite as an administrator. Mr. Weber's attempts to log in to the Confluence virtual server, Bamboo virtual, Stash server, and Jira server, were unsuccessful, and he was unable to elevate his user privileges to administrator privileges on each of the Atlassian products. (Tr. 1408).

On Monday, April 18, 2016, Mr. Leonis sent an email to all AED and ISB personnel informing them that, over the weekend, "ISB/SED personnel transferred all system admin

responsibilities across all Atlassian products to SED/ISB – removing local admin rights from all local AED branch system admins." (GX1064 at 1).

5. April 18 and 19, 2016: Schulte is Admonished for Self-Granting Revoked Privileges and Continues Testing His Accesses to DevLAN

The morning of April 18, 2016, Mr. Leonis and a human resources officer spoke to Schulte about Schulte's abuse of his Atlassian administrator privileges on April 14. Mr. Leonis gave Schulte a memorandum, "Self-Granting Previously Revoked Admin Privileges on an Agency Computer Network." (Tr. 525-28). The memorandum summarized Schulte's abuse of his Atlassian administrator privileges, noting that, upon learning he was removed as an administrator of the OSB Libraries project on April 14, 2016, and after having discussed the matter with both Sean and Mr. Weber, Schulte said that he "will eventually get access back to the libraries and that [his] access should just be enabled now." (GX1095). Schulte claimed that his statement was "I am adding my access back, until some[one] with authority advises me otherwise," and asked that his version of events be added to the memorandum. (*Id.*; Tr. 528). Schulte also claimed that, after speaking with Mr. Weber, Schulte viewed his removal form the OSB Libraries administrators as "unauthorized."[5] (GX1095; Tr. 529). The memorandum went on to state that "Administrative Rights are provided to trusted individuals for the sole purpose of ensuring that the right people have access to data in order to complete job-related tasks," and that "the OSB Libraries (and any associated computer

[5] Schulte's false version of events was contradicted by (1) Mr. Weber's subsequent email to Schulte, copying Sean and Mr. Leonis, reiterating that, having discussed the matter with Sean, Schulte's access to OSB Libraries would remain as a user (GX1061 at 5); and (2) Schulte's reply email asking to continue his prior role with OSB Libraries. (*Id*. at 4). Schulte never claimed that his removal from the OSB Libraries administrators was unauthorized, and only after Mr. Leonis responded by describing how the libraries would be moved to JoJo's supervision, without granting Schulte's request to remain an administrator (*id*. at 3-4), did Schulte restore his OSB Libraries administrator privileges.

network exploitation (CNE) related code libraries, development tools, etc.) will be administered by designated AED/OSB personnel until further notice. Please do not attempt to restore or provide yourself administrative rights to any project and/or system for which they have been removed." (GX1095; *see also* GX1066).

At approximately 11:08 a.m. and 11:13 a.m. on April 18, Schulte unsuccessfully attempted to log in to the Confluence virtual server as an administrator using both his SSH key and a username/password. (GX1703-1 at 31, 1207-26; Tr. 839-40). In between these attempts, at approximately 11:12, Schulte attempted to log in to the OSB server using his SSH key, which was successful. (GX1703-1 at 32, GX1209-17; Tr. 841-42). At that point, Schulte had two root, or administrator, sessions open on the OSB server—the root session that he had opened the Friday before, on April 15; and the new root session that he opened on the morning of April 18. Schulte would close the April 18 root session later that afternoon, at approximately 1:47 p.m. (GX1703-1 at 32, GX1209-20; Tr. 842). By opening a new root session, Schulte was able to test his SSH access without closing his existing root session—which, if his SSH key had been removed from the OSB server, would have cut off his clandestine administrator access to the server.

At approximately 12:29 p.m. on April 18, Schulte emailed Mr. Leonis, stating, "I verified that all private keys with access have been destroyed/revoked." (GX1063). Schulte complained about "how suddenly everything occurred and without notice to me," and claimed that "overnight (literally) all my permissions within the products were removed and all my permissions on the servers themselves revoked…All without anyone informing me." (*Id.*). At the time Schule claimed "all private keys with access have been destroyed/revoked" and "all my permissions on the servers themselves revoked," he was logged into two simultaneous root sessions on the OSB server using his SSH key. His email did not disclose these root sessions to Mr. Leonis.

Schulte not only had an open root session on the OSB server, but he used it. In the evening of April 18, 2016, Schulte spent approximately an hour and 20 minutes, from approximately 6:08 to 7:29 p.m., using his root session or review and edit log files on the OSB server and review the contents of the Confluence virtual server folder. Deleted files forensically recovered from a Linux virtual machine on Schulte's workstation—the VM from which Schulte opened his OSB server root session—show that Schulte listed files in various folders on the OSB server and executed commands to view and permit editing of particular log files. (GX1703-1 at 36, GX1203-43; Tr. 845-46). Command lines recovered from "file slack," or deleted portions, of a log file named "shell.log"[6] on the OSB server—indicative of Schulte having deleted those commands from the log file—also show Schulte listing files in multiple folders on the OSB server and opening log files to view and potentially edit them. (GX1703-1 at 37, Tr. 846-47). Schulte deleted (the "rm" command) a log file named "vpxa.16" (GX1703-1 at 37, GX1209-8) and viewed the contents of the Confluence folder (GX1703-1 at 39; Tr. 849), which would have shown, among other things, the "bkup 4-16-2016" snapshot of the Confluence virtual server—the snapshot taken before Schulte's Confluence administrator privileges were removed on April 16.

Also on April 18, 2016, Schulte ran internet searches about copying files over a Linux system, copying large files over a Linux system, copying multiple files over a Linux system, copying large files quickly over a Linux system, and "hashing" large files copied over a Linux system. (GX1704-1 at 33, GX3501-1; Tr. 1148-49). "Hashing" is a method of comparing two computer files to determine if they are identical, and can be used to ensure that a file copied

[6] The "shell.log" file on the OSB ESXi server recorded all commands run on the OSB server. (Tr. 761, 850). Commands recovered from the file slack of the shell.log file were deleted by Schulte when he edited the shell.log file. (Tr. 761-62, 850-51).

correctly and without any errors or data loss. (Tr. 1148). The Atlassian products were installed on a Linux system (Tr. 1371) and the OSB ESXi server was a Linux system. (Tr. 740). The next day, April 19, 2016, Schulte continued researching file hashing, running multiple internet searches between approximately 11:36 a.m. and 11:36 p.m. (GX1704-1 at 34, Tr. 1148-49).

6. April 20, 2016: Schulte Learns That Confluence Would Be Moved From the OSB Server and Copies the Atlassian Backups

On Wednesday, April 20, 2016, Schulte learned that the Confluence virtual server would be moved from the OSB's server to ISB infrastructure. At approximately 12:06 p.m. on April 20, Mr. Weber sent an email to EDG personnel that ISB was migrating Confluence and Bamboo to new computers and those virtual servers would be unavailable during the move the following Monday, April 25. (GX1067). Later that day, at about 3:58 p.m., Robert—the chief of ISB—sent an email to the same users further clarifying that the Confluence and Bamboo virtual servers would be transferred "to new servers/hardware to bring the DevLan Atlassian Suite under SED/ISB configuration mgmt. in accordance with EDG best practices." (GX1069). Moving the Confluence virtual server from OSB's server would eliminate Schulte's ability to use his secretly retained root session to manipulate the Confluence VM.

Schulte acted quickly—that same day. At approximately 5:29 p.m., after the end of the usual AED workday, Schulte began using his OSB server root access. First, he listed log files on the server (GX1703-1 at 47-49, GX1203-1, GX1203-2; Tr. 858-61), then viewed available snapshots in the Confluence folder. (GX1703-1 at 49, GX1201-16; Tr. 862). The April 16, 2016, snapshot was among those. (*Id.*; GX1703-1 at 50). Schulte then took his own snapshot of the Confluence virtual server, named "bkup," thus preserving the state of the server as it existed before he began manipulating it. (GX1703-1 at 51 & 53; Tr. 862-64).

Schulte then reverted Confluence to the April 16, 2016 snapshot, "bkup 4-16-2016." The reversion completed at approximately 5:35 p.m. (GX1703-1 at 54-55, GX1202-18; Tr. 864-65). With the Confluence virtual server reverted to its April 16, 2016 state, Schulte's administrator access to the Confluence VM was restored. (Tr. 866-67). Schulte used his restored Confluence administrator access to navigate to the Altabackup directory. At 5:42 p.m., the March 3, 2016, Confluence backup files were modified, reflecting Schulte's copying the files. (GX1703-1 at 66, GX1207-27, GX1207-30; Tr. 871).[7] During this time, Schulte copied the Confluence and Stash backup files from March 3, 2016 (the "Backup Files").

At approximately 6:51 p.m., after the Confluence server had been reverted to its April 16, 2016 state for almost an hour and a half, Schulte restored the server to its April 20, 5:29 p.m. state by re-reverting to his "bkup" snapshot. (GX1703-1 at 61, GX1202-19; Tr. 867-68). The server warned that the "current state of the Virtual Machine will be lost unless it has been saved in a snapshot." (GX1703-1 at 61). Schulte started the reversion without saving the current state of the Confluence virtual server, effectively deleting all records of his activities within the Confluence virtual server during the time it was reverted to its April 16, 2016 state. (Tr. 868-69, 872, 893). The destroyed records include records of the commands that Schulte entered from within the Confluence virtual server to initiate the file copy and transfer of the Backup Files from the Altabackup directory, which he could only do from inside the Confluence VM. (Tr. 1083-84).

[7] By the time WikiLeaks began publishing data from the stolen files, the March 3, 2016 Stash backup files had been deleted from the system due to their age, so there the date-modified information for the March 3, 2016 Stash backups was unavailable. (GX 706; Tr. 775-77, 1163). As discussed below, forensic analysis of the Stash files released by WikiLeaks showed that they came from the March 3, 2016 Stash backup files.

Schulte then searched for available Confluence snapshots and deleted the snapshot that he took at 5:29. (GX1703-1 at 63-64, GX1202-20, GX1202-21; Tr. 869-70).

Evidence of Schulte's intensive efforts to locate and delete any log files that he could find, however, was recovered, principally from unallocated space on the virtual machine Schulte used to open his root session on OSB's server from his CIA workstation. (GX1703-1 at 68-90). That these records were recovered from unallocated space indicates that Schulte deleted them in an attempt to destroy evidence of his activities. (Tr. 762-63). This forensically recovered data showed that, between approximately 5:55 p.m. and 6:58 p.m., Schulte repeatedly searched for log files on the OSB server, opened log files for editing, and deleted log files. (GX1703-1 at 69-90). Schulte targeted particular log files that record specific types of activity and all log files that had been updated most recently—the log files containing information from the evening of April 20, 2016. (Tr. 854-56, 874-91). This pattern of log file deletion is reflective of unauthorized computer intrusions and incompatible with ordinary system administration. (Tr. 857, 1089, 1379-81, 1624).

Schulte also attempted to find log files called "viclient" on the OSB ESXi server, but failed because those files were on his workstation. (GX1703-1 at 78; Tr. 873, 880-82). The viclient log files recorded Schulte's commands to list the available snapshots of the Confluence virtual server at 5:29 p.m., create the "bkup" snapshot, revert the Confluence virtual server to the April 16 snapshot, re-revert the Confluence virtual server to the 5:29 "bkup" snapshot, list again available Confluence snapshots, and delete his "bkup" snapshot. (GX1703-1 at 49, 51, 54-55, 61, 63-64).

At 7:07 p.m., Schulte closed the vault where RDB was located and armed the alarm, showing that he was the last person to leave the vault that evening. (GX107; Tr. 892).

7. Schulte Transmits the Stolen CIA Files to WikiLeaks and Securely Deletes Data From His Home Computer

Between April 18 and May 5, 2016, Schulte took a number of steps that he would need to transmit the Backup Files to WikiLeaks, and then securely deleted all data from his home computer to eliminate the evidence of his transmittal.

The WikiLeaks website available in April of 2016 offered instructions and guidance on submitting documents to WikiLeaks, which lined up precisely with Schulte's actions as he was preparing to steal the Backup Files and in the weeks following his theft. WikiLeaks's submissions page could only be access through Tor ("The Onion Router"), "an encrypted anonymizing network that makes it harder to intercept internet communications, or see where communications are coming from or going to." (GX1704-1 at 38-41; Tr. at 1104-05). It is very difficult to recover forensic artifacts of a user's activities using Tor. (Tr. 1309-11). Schulte updated the version of Tor on his home computer on April 18, 2016 (DX1409, lines 4873-8000; *see also* GX1704-1 at 52; Tr. 1105-06, 1313), the same day that he was admonished for abusing his administrator privileges and learned that his Atlassian administrator privileges had been revoked. *Supra* 12-13.

WikiLeaks advised those who "are at high risk" to use Tails, an operating system that boots from an external media device and is designed to leave no forensic traces of the user's activities. (GX1704-1 at 42-45; Tr. 1106-08). The Tails operating system automatically connects to Tor so that all of the user's internet activity occurs over the Tor network. (Tr. 1108). Schulte downloaded the then-current version of Tails on his home computer on April 24, 2016 (GX1704-1 at 51, GX1403-7; Tr. 1109-10), a few days after his theft of the backup files. The use of Tails reduces or eliminates forensic artifacts of the user's activity. (Tr. 1308-09).

WikiLeaks also advised "high-risk" sources to "format and dispose of the computer hard drive and any other storage media you used." WikiLeaks cautioned that "hard drives retain data

after formatting which may be visible to a digital forensics team . . . .” (GX1704-1 at 50). Between April 23 and May 4, 2016, Schulte researched, downloaded, and tested various methods of secure data deletion. (GX1704-1 at 58-69). Ordinary deletion commands, and even ordinary disc formatting, do not remove the underlying data from the storage media. (Tr. 1111-14, 1120-22, 1176). There are secure data deletion utilities and disk wiping utilities that overwrite the underlying data, making it difficult or impossible to recover the overwritten data. (*Id.*). Schulte tested one such secure file-deletion utility called Eraser Portable between April 23 and 28, 2016. Schulte securely deleted folders called “Brutal Kangaroo” (the name of an EDG tool suite) and “Array List,” and queued backup files named “data.bkp,” “data2.bkp,” “data3.bkp,” “data4.bkp,” “data5.bkp,” and “data6.bkp” for secure deletion but quit the application before deleting those files. (GX1704-1 at 58-63, GX1404-1, GX1404-2, GX1404-15; Tr. 1166-67).

On April 30, 2016, Schulte downloaded Darik’s Boot N Nuke (“DBAN”), a secure disk-wiping facility. (GX1704-1 at 64, GX1402-8; Tr. 1167). Between April 30 and May 4, 2016, Schulte conducted several internet searches relating to secure data deletion and disc wiping (GX1704-1 at 69, GX1305-9; Tr. 1175).[8] Schulte then wiped and reformatted his home computer’s internal hard drives on or about May 5, 2016. (GX1704-1 at 72 & 73; Tr. 1173-77. 1311-12, 1315). Schulte also had several external hard drives that had been wiped before being seized by the FBI during the search of his apartment. (GX 1608-1615; Tr. 1167-69, 1315). The effect of using Tor, Tails, and secure data deletion and disc wiping utilities was to destroy the forensic artifacts directly showing Schulte’s transmission of the Backup Files to WikiLeaks. (Tr. 1314-15).

[8] In the same time period, on May 1, 2016, Schulte researched hash algorithms, which are used to ensure data transfers or copies are error-free, just as he did in preparation for copying the backup files off the DevLAN network. (GX1704-1 at 68, GX1305-8; Tr. 1170-71).

8. Schulte Resigns From the CIA Amid Further Disgruntlement

Schulte resigned from the CIA in November 2016, six months after stealing the Backup Files. In the interim, he continued to claim that his administrator privileges had been wrongly revoked, allege that he had been retaliated against, and abuse his remaining network privileges.

For example, on May 26, 2016, Schulte falsely claimed Mr. Weber's removing Schulte from the administrators of the OSB Libraries Stash project was unauthorized and that Schulte was not informed of his removal until after his Atlassian administrator privileges had been revoked. (GX1080). Around this time, Schulte was given administrator privileges to one of his former OSB projects, called Brutal Kangaroo, and then abused that access to remove all of the OSB administrators. (Tr. 548-57).[9] When EDG's leadership restored privileges to the Brutal Kangaroo Stash project to their prior status, Schulte claimed that his privileges were being removed unfairly and that he would "fight back." (Tr. 556-58).

Schulte escalated his grievance to the chief and deputy chief of CCI, embellishing his false narrative of being the victim of retaliation. (GX1093). Schulte also repeated his false claims about his OSB Libraries administrator status being wrongly revoked, claiming that he had restored his OSB Libraries privileges before speaking with Mr. Weber, that Mr. Weber had made the change because of Mr. Weber's unhappiness with Schulte's administration of OSB Libraries rather than any OSB or AED management decisions, and that Sean had denied giving Mr. Weber permission to change Schulte's privileges. Sean Roche, then the deputy chief of CCI, immediately arranged a meeting with Schulte. (GX1096; Tr. 1668-72). Schulte's elevation of his own privileges on CIA

[9] The Brutal Kangaroo project included a tool called Shattered Assurance, which Schulte took with him to RDB. Schulte did not need administrator privileges to the Brutal Kangaroo Stash project in order to continue his work on Shattered Assurance. (Tr. 556-57).

networks was a serious security matter (Tr. 1667) and Mr. Roche reminded Schulte that officers had been removed from the CIA for similar conduct. (Tr. 1676-77). Schulte responded, "I could restore my privileges if I wanted to, you know I could do that." (Tr. 1677).

Later, in a July 19, 2016, interview with security personnel about Schulte's allegations against Amol, Schulte repeatedly reiterated his false claims about being removed as administrator of the OSB Libraries Stash project. (GX509-2, GX509-2T at 3-4; *see also* GX509-3T at 9-12). Schulte asserted that: "I'm the site administrator overall. So access doesn't really apply to me, essentially, it how it works. So--so I can get--they go through and remove my permissions from stuff, but I still have full permission to everything, right?" (GX509-2, GX509-2T at 3-4).

In the late summer and early fall of 2016, WikiLeaks had not yet published material from the Backup Files. Schulte began searching for news and information relating to WikiLeaks on an increasingly frequent basis (GX1351, GX1352; Tr. 260-61), reflecting his concern about the delay in publication and his hope that the Backup Files would be disclosed.[10]

9. March through October 2017: WikiLeaks Publishes Classified Materials From the Backup Files

On March 7, 2017, WikiLeaks began publishing classified data from the Backup Files. (GX1). Between March and November 2017, there were a total of 26 disclosures of classified data from the Backup Files, which WikiLeaks denominated as Vault 7 and Vault 8 (the "WikiLeaks Disclosures"). (Tr. 108, 112, 473-75, 1363-64, 1650-51).

[10] Due to an error in the script that created the backups, the Confluence backup files were corrupted and some of the data was lost. (Tr. 778-80). FBI forensic examiners were able to manually reconstruct portions of Confluence from the backups, but the process was time consuming and the results incomplete. (Tr. 780-84). WikiLeaks would have needed to similarly reconstruct Confluence pages, which likely accounts for the length of time between Schulte's transmitting the Backup Files to WikiLeaks and the beginning of WikiLeaks' disclosures.

The impact on the CIA was immediately catastrophic. DevLAN was disconnected and the network and every external device connected to it were seized by the FBI. (Tr. 572-74, 1365; *see also* Tr. 130-31). EDG personnel had no computer equipment for cyber development. (Tr. 1365). A number of EDG personnel diverted their resources from developing tools for cyber operations to assessing the extent of the intrusion and the risk and impact of additional disclosures. (Tr. 572-73, 1364). Further cyber operations were halted and previous and ongoing operations were at risk of exposure. (Tr. 575, 1366-67, 1651-52, 1686). EDG tools had to be rebuilt and redesigned. (Tr. 478, 575, 1364). The effect of the WikiLeaks Disclosure was a "digital Pearl Harbor. We were dead in the water." (Tr. 1681; *see also* Tr. 112-13).

10. Schulte Obstructs the WikiLeaks Investigation

The FBI considered a broad range of potential suspects in its investigation of the WikiLeaks Disclosures, but Schulte was quickly identified as likely being involved based on his history of abusing administrator privileges and his animosity towards the CIA. (Tr. 129, 173-75).

On March 14, 2017, the FBI approached Schulte as he was leaving work at Bloomberg in New York, where he had moved after leaving the CIA, and asked to speak with him. (Tr. 205-206). During a voluntary interview at a nearby restaurant, Schulte denied being responsible for the WikiLeaks Disclosures. (Tr. 210). At the conclusion of the interview, Schulte was given two grand jury subpoenas. (Tr. 210-11). One subpoena required Schulte's appearance before the grand jury on March 17, 2017; and the second required Schulte to produce his cellphone. (Tr. 210).

After being served with the two subpoenas, Schulte told the agents that he had travel plans. (Tr. 211). The FBI had learned earlier that Schulte was issued a diplomatic passport while employed by the CIA and that Schulte had failed to return the passport when he resigned. (*Id.*). Schulte claimed that the diplomatic passport was at his apartment. (Tr. 212). The agents accompanied Schulte to his apartment, where a team was waiting to execute a search warrant. (*Id.*).

Schulte agreed to unlock his apartment door, and when asked if there were any emails from his time at the CIA or any classified information inside, said there were none. (Tr. 212-13). Printed emails from Schulte's employment and documents containing classified information, including documents with the true names of CIA employees operating under cover, were in fact recovered from the apartment, including from a storage compartment in Schulte's headboard. (GX1616-1619; Tr. 213, 223-26). The FBI had specifically asked Schulte about one of the recovered emails, and Schulte had denied possessing a copy. (GX1616; Tr. 223, 428-29). Schulte's paper shredder contained shreddings from additional CIA emails, including emails with CIA officers' true names. (GX1621, 227-230).[11] The diplomatic passport was not in the apartment. (Tr. 213).

Schulte left the apartment as the search was underway, and FBI surveillance observed him return to Bloomberg. (*Id.*). The agents told Schulte that classified documents had been found in his apartment, and that the diplomatic passport had not. (Tr. 213). When asked again about the passport, Schulte admitted it was at his office desk. (Tr. 214). FBI agents accompanied Schulte to his desk and retrieved the passport. (*Id.*).

Though served with a grand jury subpoena, Schulte was not ultimately called to appear before the grand jury. Instead, he participated in voluntary interviews with attorneys on March 20 and 21, 2017, at the U.S. Attorney's office with FBI agents and Assistant United States Attorneys. (Tr. 231-32). During these two days of interviews, Schulte described ways that the WikiLeaks Disclosures could have been obtained from CIA computers. (Tr. 232). Two of Schulte's proposed methods were to individually copy Confluence pages or to access offsite backup servers—methods

[11] The emails containing classified information generally contained classification banners misclassifying the contents as "unclassified." Most of those classification designations were made by Schulte as the sender of the emails. (GX1616, GX1618, GX1621; Tr. 246-49).

very dissimilar to how Schulte actually stole the Backup Files. A third method was to access the onsite backups, either physically—again, dissimilar to Schulte's actual theft—or from a CIA desktop computer. (*Id.*). Schulte stated that the CIA computer system kept log files that might show activity that would identify the leaker (Tr. 234), but did not disclose that Schulte himself had deleted and attempted to delete any log files that would contain that information. Schulte said that when he was an administrator on the system, he would access the backup folder using the Stash server. (Tr. 233). Schulte denied making the CIA system vulnerable to compromise, denied providing information to WikiLeaks, and denied having any involvement in the leak. (Tr. 234-35).

11. Schulte Continues His Efforts to Leak Classified Information From Prison As Part of an "Information War" Against His Prosecution

Schulte was ultimately arrested and, during 2018, detained pending trial at the Metropolitan Correctional Center ("MCC") in Manhattan, New York. In the summer and fall of 2018, Schulte made plans to wage an "information war" against the United States government to influence his criminal case through the media and to retaliate against his prosecution and perceived grievances against the CIA. In furtherance of this campaign, Schulte obtained access to contraband cellphones (Tr. 1712-20) that he used to create anonymous, encrypted email and social media accounts. (GX820-434 & -436; GX823; GX1303-11, -44, -50, & -63; Tr. 1752, 1831-35, 1853-57).

Schulte documented his planned campaign in handwritten journals. In an entry dated August 8, Schulte wrote: "If govt doesn't pay me $50 billion in restitution & prosecute the criminals who liked to the judge and presented this BS case then I will visit every country in the world and bear witness to the treachery that is the USG [United States government]. I will look to breakup diplomatic relationships, close embassies, end U.S. occupation across the world..." (GX809 at 2). On August 14, Schulte wrote: "Got to use last night," referring to a contraband cellphone; "[t]he was is clear. I will set up a wordpress … From here, I will stage my information war." Schulte wrote about releasing posts

and articles on social media as he wrote them. (GX809 at 3). In an "article" Schulte was writing about his various grievances against the government, he wrote: "The FBI, in all its brilliance, has just taken a senior engineer with intimate knowledge of the NSA, CIA, and all projects and operations he's worked on … Does that sound like the most intelligent mover, really? Obviously this isn't intended as a threat … Essentially, it's the same as taking a soldier in the military, handing him a rifle, and then begin beating him senseless to test his loyalty and see if you end up getting shot in the foot or not. It just isn't smart." (GX820-430 & -431).

Schulte continued to document his plans in an entry dated August 21st, a checklist of actions for furthering his information war, avoiding detection, and deleting evidence. (GX809 at 5). Schulte's list included deleting emails and documents from one of his anonymous accounts (johnsmith); creating new logins and passwords for accounts; creating a new encrypted email account; setting up new WhatsApp, Signal, and Telegram accounts with different phone numbers; resetting his contraband cellphone and cleaning off the apps; and changing the IMEI associated with his Samsung contraband cellphone. (*Id.*). Schulte learned that the FBI had learned the IMEI of one of his other cellphones by subpoena, and worried that the IMEI could be used to identify his accounts. (*Id.*). That following day, Schulte used a random password generator to create new passwords for his email and social media accounts. (GX809 at 6; Tr. 1833-34).

On August 23, 2018, Schulte wrote about transitioning to his new encrypted email accounts and cleaning the contraband cellphone. (GX809 at 7). Schulte also noted that he had started emailing a reporter from the Washington Post. (*Id.*). Using a messaging app and an anonymous email account, Schulte communicated with the reporter about his prosecution, pretending to be one of his own family members and a friend of the family. (GX812, GX822-1). In an email dated September 24, 2018, Schulte emailed the reporter a search warrant affidavit that had been produced in discovery subject to a protective order, along with Schulte's comments on the affidavit.

Schulte's criticisms of the affidavit's allegations included classified information about the DevLAN network and the number of employees in EDG and its sister group within CCI, COG.[12] (GX812 at 3; Tr. 1670-71). In addition to emailing the reporter, Schulte attempted to use the contraband cellphones to transmit his discovery materials to WikiLeaks, but was unable to. His journal entry for September 12, 2018 includes the note, "DL disc UL WL," meaning "download discovery, upload to WikiLeaks." (GX809 at 15; *see also* Tr. 1754-56, 1799-1801).

Throughout August and September, Schulte drafted blog posts and tweets. In these, Schulte pretended to be one of his own former CIA colleagues and falsely claimed his innocence. (GX809 at 8-13). These draft tweets and blog posts contained classified information about CIA cyber tools and operations. Schulte sought to authenticate his assumed identity as a CIA developer by revealing information about a particular cyber tool called Bartender, including details of Bartender's operation and information that would publicly associated Bartender with an piece of malware that had been found by security professionals but had never been attributed to the CIA. (GX809 at 8, 10, 11; Tr. 1421-28, 1604-05, 1653-55). Schulte's writings also reflect his desire to leak and cause the leak of classified information, such as hashtags "#TopSecret" and "#FuckYourTopSecret" (GX809 at 11) and exhortations to government employees to "send all your govt's secrets here: WikiLeaks." (GX809 at 13).

On September 12, 2018, Schulte wrote about finalizing copy, referring to his blog posts and articles; and scheduling tweets. Schulte in fact had created a Buffer account, an application for scheduling tweets or Facebook posts (Tr. 1858), and had linked his Twitter account, "@freejasonbourne," to the Buffer account. (DX815). One of Schulte's articles, called Article 10

[12] COG was a group at CCI that was often responsible for deploying cyber tools developed by AED or working with an asset who would deploy the tool. (Tr. 1361).

or Malware of the Mind, included a description of CIA cyber tool techniques for concealing data. (GX801). The FBI searched Schulte's MCC cell and seized the contraband phones on October 3, 2018, before Schulte publicly released his blog posts and tweets. (Tr. 1813-14).

B. The Defense Case

Schulte called three witnesses: Hannah Sotnick, a former paralegal on his defense team, who testified that Schulte gave her a copy of Malware of the Mind, which Ms. Sotnick delivered to one of Schulte's attorneys (Tr. 1977-79); Cheng, a former colleague of Schulte's at RDB who had also worked at the NSA, and who testified that NSA had heightened network security protocols compared to those in place on DevLAN (Tr. 1985-90); and Dave, a systems administrator with ISB, who testified about various security practices and network permissions on DevLAN. (Tr. 1994-2026). Dave testified about various characteristics of DevLAN, including that monitoring was in place to detect if DevLAN users connected their DevLAN workstations to the internet (Tr. 1995-96); that developers were administrators with respect to their individual workstations (Tr. 1994); that individual users controlled access to their home directories on the network, with the default setting that only the user had access to their folder (Tr. 1998-2005, 2018-); the Dave had at one time copied a Stash backup to his own home directory, which was set to preclude access from any other users (Tr. 1998, 2019); that Dave made a different backup copy of Stash on an external hard drive on April 16, 2016, at Mr. Weber's request (Tr. 2005-09); that the external hard drive was stored in a safe or a locked drawer in Dave's desk until it was most likely destroyed, though Dave did not specifically recall (Tr. 2007-13); that in April 2016, ISB copied the Confluence virtual server from OSB's server to a staging directory of OSB and then to an ISB ESXi server (Tr. 2013-15, 2021-23); and that ISB could access users' desktops

remotely for troubleshooting using Remote Desktop Protocol if the user accepted the remote connection (Tr. 2016-17, 2023-24).

III. The Verdict And Rule 29 Motion

On July 17, 2022, the jury found Schulte guilty on all counts.

After the Government rested following its case-in-chief, Schulte moved pursuant to Rule 29 for a judgment of acquittal. (Tr. 1947-57). With respect to Counts Two, Three, and Four, Schulte argued principally that the evidence was insufficient to show that he had transmitted or attempted to transmit documents relating to the national defense, as opposed to information under § 793(e); and that the "information" prong of the statute requires the Government to show that the defendant had reason to believe the information could be used to the injury of the United States or to the advantage of a foreign nation. The Court reserved judgment on that issue. (Tr. 1947-52). Schulte also argued, with respect to Counts Five, Six, Seven, and Eight, that the evidence failed to prove that any computer access was unauthorized because of his SSH key access to the OSB ESXi server root session. The Court denied that aspect of the defendant's motion. (Tr. 1955-57). Schulte generically moved for a judgment of acquittal on the remaining counts. (Tr. 1957).

On January 12, 2023, Schulte filed his *pro se* Motion for a judgment of acquittal pursuant to Rule 29 or for a new trial pursuant to Rule 33. In the Motion, Schulte argued that:

(1) the evidence at trial was insufficient with respect to Counts Three and Four, charging the unlawful transmittal and attempted transmittal of documents containing national defense information ("NDI") from the MCC, because the documents did not contain NDI, the information was not unlawfully possessed, the transmitted material consisted of information rather than documents, and the transmission was not willful (Mot. 2-24);

(2) the evidence was insufficient with respect to Counts Seven and Eight, charging the unauthorized access of CIA computer systems to obtain classified information and to cause

harmful computer commands, because Schulte's access to CIA computer systems was authorized and because Schulte did not intend to and did not cause damage or harmful consequences to those systems (Mot. 25-34);

(3) the evidence was insufficient as to Count Nine, charging the obstruction of a grand jury proceeding, because Schulte did not know of any pending grand jury proceedings, he did not know his statements would affect a grand jury, and he did not lie (Mot. 35-38);

(4) the evidence was insufficient as to Counts One, Two, Five, and Six, charging the unlawful gathering of NDI from CIA computer systems and unlawful transmission of NDI to WikiLeaks, because there was no evidence that Schulte gathered NDI, no evidence of copying NDI, no evidence of Schulte connecting removable media to CIA computer systems to copy NDI, no evidence of Schulte possessing NDI at his home, no evidence of transmission to WikiLeaks, and no evidence of access controls to the Backup Files (Mot. 39-75);

(5) a new trial is required because Schulte was not provided access to a complete copy of the entire DevLAN network, including offsite backup storage, international network components, and all connected computers and devices (Mot. 76-107), which the Court has previously denied pursuant to the Classified Information Procedures Act ("CIPA") (D.E. 124, 514, 823); and

(6) a new trial is required because Schulte was not give access to a particular CIA report (Mot. 108-09), which does not exist (D.E. 591), and because of purportedly prejudicial statements by the Government during jury addresses (Mot. 109-11).

ARGUMENT

I. THE EVIDENCE WAS SUFFICIENT TO SUSTAIN THE JURY'S VERDICT

The proof at trial was more than sufficient to sustain the jury's verdict of guilty. Indeed, the evidence of Schulte's theft and transmittal of the Backup Files to WikiLeaks was overwhelming, as was the evidence of his continued transmittal and attempted transmittal of

classified NDI from the MCC and his attempts to obstruct the grand jury investigation of the WikiLeaks disclosures. In arguing to the contrary, Schulte consistently ignores the trial evidence, mischaracterizes evidence, argues for alternative inferences that the jury was not required to make, and argues that the Government was required to prove his crimes in particular ways with particular proof. His arguments should be rejected and the verdict upheld.

A. Applicable Law

Rule 29 provides that a "court on the defendant's motion must enter a judgment of acquittal of any offense for which the evidence is insufficient to sustain a conviction." FED. R. CRIM. P. 29(a). A defendant challenging the sufficiency of the evidence supporting a conviction "'faces a heavy burden.'" *United States v. Glenn*, 312 F.3d 58, 63 (2d Cir. 2002) (quoting *United States v. Matthews*, 20 F.3d 538, 548 (2d Cir. 1994)); *see also United States v. Heras*, 609 F.3d 101, 105 (2d Cir. 2010). "[T]he court may enter a judgment of acquittal only if the evidence that the defendant committed the crime alleged is nonexistent or so meager that no reasonable jury could find guilt beyond a reasonable doubt." *United States v. Guadagna*, 183 F.3d 122, 130 (2d Cir. 1999) (internal quotation marks omitted).

"The Court must credit every inference that the jury might have drawn in favor of the government, and review all the evidence in conjunction, not in isolation." *United States v. Baldeo*, No. 13 Cr. 125 (PAC), 2014 WL 6807833, at *1 (S.D.N.Y. Dec. 3, 2014) (internal quotation marks and citation omitted); *see also United States v. Autuori*, 212 F.3d 105, 114 (2d Cir. 2000). A conviction must therefore be affirmed if, "'after viewing the evidence in the light most favorable to the prosecution, . . . *any* rational trier of fact could [find] the essential elements of the crime beyond a reasonable doubt.'" *United States v. Pitre*, 960 F.2d 1112, 1120 (2d Cir. 1992) (quoting *Jackson v. Virginia*, 443 U.S. 307, 319 (1979)); *see also United States v. Sabhnani*, 599 F.3d 215,

241 (2d Cir. 2010); *United States v. Reifler*, 446 F.3d 65, 94-95 (2d Cir. 2006). "Accordingly, the government's case need not exclude every possible hypothesis of innocence, and where either of the two results, a reasonable doubt or no reasonable doubt, is fairly possible, the court must let the jury decide the matter." *United States v. Facen*, 812 F.3d 280, 286 (2d Cir. 2016) (quotations omitted) (citing *United States v. Martinez*, 54 F.3d 1040, 1042-43 (2d Cir. 1995) and *Guadagna*, 183 F.3d at 129. "These standards apply whether the evidence being reviewed is direct or circumstantial." *United States v. Persico*, 645 F.3d 85, 105 (2d Cir. 2011).

B. Discussion

1. Counts One and Two: The Theft of National Defense Information From the CIA and Transmission to WikiLeaks

Counts One and Two charge Schulte with violating 18 U.S.C. § 793(b) and (e) resulting from his April 20, 2016 theft of the Backup Files from the CIA, knowing that the leaked data would used to the injury of the United States or to the advantage of a foreign nation; and subsequent transmission of those electronic records to WikiLeaks. § 793(b) makes is a crime to copy, take, make, or obtain documents, writings or notes containing information relating to the national defense, with the intent or with reason to believe that the NDI was to be used to the injury of the United States or used to the advantage of the foreign country. § 793(e) makes it a crime to willfully communicate, deliver or transmit, or caused to be communicated, delivered or transmitted, documents, writings, or notes containing information pertaining to the national defense that the defendant had unauthorized possession of, to a person not entitled to receive it.

As described above, the jury was presented with overwhelming evidence that Schulte stole the Backup Files on April 20, 2016 and transmitted them to WikiLeaks. Schulte had a motive to steal the Backup Files arising on his disgruntlement with the CIA and anger over perceived, though nonexistent, instances of disrespect or unfairness. *Supra* 5-13. Schulte abused his administrator

privileges only days before, on April 14, when Schulte used his Atlassian administrator privileges to restore his status as an administrator of the OSB Libraries Stash project, s*upra* 6-7, and went on to repeatedly lie about this incident. *Supra* 12, 20. Schulte then attempted to access the Backups Files without using Atlassian administrator privileges, but was unable to. *Supra* 10. Schulte spent several days researching how to steal the Backups Files and testing his access to the network. *Supra* 9-15. Schulte's Atlassian administrator privileges were revoked on April 16, 2016, and on April 20, Schulte reverted the Confluence virtual machine to its April 16 state and thereby restored his administrator access and his access to the Altabackup directory. *Supra* 16. Schulte deleted and attempted to delete voluminous computer records recording his illicit activities. *Supra* 17. The same Backup Files that WikiLeaks later published were accessed while Schulte had the system in its reverted state. *Supra* 16. Schulte followed WikiLeaks's instructions to leakers to a "T," updating his Tor browser and Tails operating system and downloading, testing, and using secure data deletion utilities, culminating in Schulte wiping his home computer and several external hard drives in his apartment. *Supra* 18-19.

Schulte advances a host of arguments that the jury could not reasonably conclude from this evidence that he stole and transmitted the Backup Files. Schulte argues that the evidence was insufficient to permit a reasonable juror to conclude that he stole the Backup Files because (1) there was no evidence that access to the Altabackup directory was restricted, and therefore there was no reason for Schulte to engage in the complex network actions on April 20, 2016 for the purpose of stealing the Backup Files (Mot. 39-44); (2) there was insufficient evidence that the Backup Files were the source of the WikiLeaks Disclosures because a timing analysis cannot exclude the possibility that a later backup was the source (Mot. 44-46); (3) there was no forensic computer artifact reflecting a login to the Confluence virtual server, a copy command, or an external storage

device connection on April 20, 2016 (Mot. 47-54); (4) there was no evidence that the Backup Files could have been transferred during the hour and twenty minutes that the Confluence VM was in its reverted state (Mot. 54-57); (5) Schulte was in the bathroom when the March 3, 2016 Backup Files were accessed on April 20, 2016 (Mot. 57-58); (6) there was no evidence that Schulte knew he could regain access to the Altabackup directory by reverting Confluence to the April 16, 2016 snapshot (Mot. 58-59); (7) there was insufficient evidence that Schulte intended to steal the Backup Files because Schulte manually created a "transcript file" to preserve a record of his actions on the OSB ESXi server on April 20, 2016 (Mot. 59-60); and (8) there was insufficient evidence that the April 20, 2016 "date modified" for the March 3, 2016 Backup Files demonstrated that they were copied on April 20, 2016. (Mot. 61-63).[13]

Schulte's arguments rely on mischaracterizing the record, demanding that the proof conclusively exclude all other possibilities, and inventing evidence and inferences.

There was sufficient evidence of access controls to the Altabackup directory. Schulte argues "[t]he government's theory of theft relies entirely upon the predicate that the altabackups directory was locked down," and "[i]f the altabackups were not locked down, then the snapshot-reversion theory is entirely irrelevant." (Mot. 39). Schulte claims "anyone could access, copy, and steal the backups." (*Id*. 40).

There is sufficient evidence to support the jury's verdict regardless of whether Altabackup directory was "locked down" or "wide open." The defendant's reversion of the Confluence virtual server to the April 16, 2016 snapshot and re-reversion to the April 20, 2016 snapshot, without saving the state of the VM before the second reversion, deleted all records of his activities within

[13] Schulte also asserts that "the Government failed to prove elements 2 and 3 beyond a reasonable doubt" (Mot. 63) but provides no supporting argument for the assertion.

the Confluence virtual server between the two reversions and destroying evidence of his crimes. That alone would be sufficient explanation for his actions, even if Schulte could have accessed the Altabackup directory without administrator access to the Confluence virtual server.

But there was ample evidence in the record to support the jury's finding that the Altabackup directory was not "wide open" and that, without reverting the Confluence VM to its April 16, 2016 state, the defendant did not have access to Altabackup and could not steal the Backup Files. Altabackup was created by ISB in order to store backups of the Atlassian products. (Tr. 1382-83). The list of network permission for that directory—the user accounts or IP addresses that could access the directory—was not available when the FBI investigated of the WikiLeaks leak. (Tr. 815). But there was ample other evidence that ordinary users could not access Altabackup. Mr. Weber, an Atlassian administrator until April 16, 2016, testified that he accessed the Altabackup directory from the Confluence virtual server (Tr. 1600)[14] and that he did not have authority to access the Altabackup directory after Atlassian administrator privileges and responsibilities were transferred to ISB. (Tr. 1410). Schulte himself told the FBI that he accessed the Altabackup directory from the Stash server. (Tr. 233). Significantly, on April 15, 2016, Schulte attempted to create a datastore—a type of mount point—to the Altabackup directory from a user session on OSB's ESXi server, and permission was denied. (GX1703-1 at 12-13, GX1202-7, GX1202-8; Tr. 813-15). The network denial message stated: "The mount request was denied by the NFS [network file system] server. Check that the export exists and that the client is permitted to mount it."

[14] Schulte claims Mr. Weber accessed the Altabackup directory from his workstation (Mot. 43, Tr. 1524), but that testimony does not support Schulte's argument. Mr. Weber, like Schulte, accessed the Confluence VM from a login session on his workstation. (Tr. 1372). Viewing the testimony as a whole, it is clear that he accessed the Altabackup directory from an administrator Confluence session.

(GX1703-1 at 13, GX1202-8). Mr. Leedom, an expert in digital forensics and computer science, testified that it was standard for NFS servers, like the Altabackup directory, to require both a root login and an IP address on the "allow list" for access. (Tr. 952). This evidence provided sufficient basis for the jury to reasonably conclude that access to the Altabackup directory required Atlassian administrator access to one of the Atlassian servers, like the Confluence virtual server, which was on the "allow list" in order to write backup files to the Altabackup directory.

Schulte's actions on April 20, 2016 reflect his own understanding that access to the Altabackup directory was restricted, and further support the jury's reasonable conclusion. There is no dispute that the Confluence virtual server had a mount point to the Altabackup directory, so that it could save backups to that directory. There is no dispute that, after Schulte's Atlassian administrator privileges were revoked on April 16, he could no longer log in to the Confluence virtual server; nor that, on April 20, Schulte's administrator access to the Confluence VM was restored when he reverted to the April 16 Confluence snapshot. There was no evidence supporting any other reason for Schulte's actions except to restore his access to the Confluence server and to the Altabackup directory. His reversion and re-reversion was abnormal. (Tr. 872-73 ("To get access, he had to go through this rigmarole of doing the snapshot reversions…"), 1506-07 ("[T]he more likely scenario is a snapshot is meant to be a fallback option that you don't need to fall back to if you don't want to. I created a lot of snapshots that I never reverted to.")). The purpose of a snapshot is to save the state of the system before changes are made, so that if the changes introduce errors, the system can be restored to its prior state. (Tr. 1378). There is no reason to revert to an earlier snapshot, make changes, and then revert to the state the system was in before the first reversion—any changes would only affect the earlier system state, not the current system state; and those changes to the earlier state would be lost after the re-reversion.

In sum, there was ample evidence from which the jury could conclude that access to the Backup Files was restricted and that Schulte's actions on April 20, 2016 were for the purpose of regaining his revoked access to the Altabackup directory and the Backup Files.

There was sufficient evidence that the Backup Files were the source of the data disclosed by WikiLeaks. Schulte argues that the evidence and testimony concerning the timing analysis—forensic expert analysis of which Confluence and Stash backup files were the source of the Vault 7 and Vault 8 leaks—only established a "lower bound," that is, the earliest possible backup files, but did not exclude the possibility that the leaks came from later backup files. "[T]he government simply failed to present sufficient evidence that WikiLeaks possessed the March 3, 2016 backup file—instead of any file between March 3, 2016 and March 6, 2017; no rational, reasonable juror could possibly infer that this backup, and only this backup, was provided to WikiLeaks."

Schulte's argument suffers from a lack of logic and evidentiary support. First, the evidence does not need to conclusively exclude the possibility that the stolen backups were any other than the March 3, 2016 backups, it need only support a reasonable inference that the data that WikiLeaks leaked was derived from data that Schulte stole from the CIA and transmitted. *Facen*, 812 F.3d at 286. Even if the stolen backup files were from any time between March 3 through April 20, 2016, that would still be consistent with Schulte's guilt. Second, the evidence was more than sufficient to support the conclusion that the leaked data was derived from backup files that Schulte stole, and more specifically that it came from the March 3, 2016 Backup Files.

Schulte does not dispute Mr. Leedom's conclusion that the Confluence data released by WikiLeaks came from Confluence backup files (Tr. 710, 777-96); Mr. Berger's analysis that the data released by WikiLeaks came from backup files dated no earlier than March 3, 2016 (GX1704-1 at 4-31; Tr. 1149-63); or that the March 3, 2016, Confluence backups are the only available

backups that reflect having been accessed at any point after they were created. (GX1207-27, GS1207-30; Tr. 773-75, 1162-63). That is more than sufficient to support the inference that the March 3, 2016, backup files were stolen by Schulte and that they were the source of the WikiLeaks Disclosures. In addition, Mr. Leedom testified that it is not feasible, notwithstanding version control, to use a later backup to mimic a prior backup. (Tr. 797-98). "There is no way you would really be able to know just from what is there what it would have looked like on March 3rd." (*Id.*). Schulte simply ignores this testimony.

There was sufficient evidence that Schulte destroyed data reflecting his Confluence virtual server login, copy command, and any external storage device connection. In the Motion, Schulte argues (as he did during his closing at trial) that the Government failed to prove its case because "the government has a perfectly intact detailed picture of all the activity from Mr. Schulte's CIA Workstation" on the evening of April 20, 2016, and "[t]here was no command to log into the Confluence VM nor any commands to copy any file from it." (Mot. 47-48; *see also* Tr. 2188, 2204, 2208-10, 2215). In a similar vein, Schulte argues that "no removable drive, hard drive, or anything was ever connected into Mr. Schulte's CIA Workstation during the Confluence reversion." (Mot. 53; *see also* Tr. 2210-11). Schulte argues that, without these forensic artifacts, the jury could not reasonably have reached a verdict of guilty. (*See generally* Mot. 47-54).

Schulte bases these arguments on a false characterization of the record. He claims that the FBI recovered a perfect record of his activities on April 20 in the form of a "transcript file." The FBI did not recover a perfect record of his activities, because Schulte deleted scores of log files and edited other log files to delete particular records of his activities. Schulte also reversed his reversion of the Confluence virtual server from the April 16, 2016 snapshot to his April 20, 2016 snapshot without saving the state of the system, resulting in the complete deletion of all of his

activities inside the Confluence server while it was in its April 16 state. The log files that Schulte deleted and the lost data from the Confluence reversion include the precise files that Schulte focuses on: his Confluence server login, his commands to copy the Backup Files, and records of external storage device connections to the network. (GX1703-1 at 72-73, 84; Tr. 876-78, 886-87).

Schulte relies heavily on what he calls a "transcript file" or "transcript log," which, according to Schulte, "logged every single command Mr. Schulte ran from his computer—including commands to log into remote computers and execute commands on those remote computers." (Mot. 48). Schulte is incorrect—there was no evidence of any completely intact "transcript file" or "transcript log," or any evidence of a single log file that recorded all of his activities on April 20. The evidence of Schulte's actions on the network were found in several different places: from unallocated space on the OSB ESXi server (that is, deleted file space) (*e.g.*, GX1703-1 at 5); file slack (that is, deleted command lines) from the shell.log file on the OSB ESXi server (*e.g.*, GX1703-1 at 37, 39), viclient log files from Schulte's workstation (*e.g.*, GX1703-1 at 12, 13, 49, 51, 53, 54, 61, 63, 64), and unallocated space on Schulte's workstation (that is, deleted file space) (*e.g.*, GX1703-1 at 20, 36, 38, 46, 47, 69, 71, 75, 76, 78-81, 83, 86, 88-90).

What Schulte mischaracterizes as a "transcript file" is deleted data from the virtual machine on Schulte's workstation he used to log in to the OSB server. Mr. Leedom explained:

> Q: Did you find any actual transcript files on Mr. Schulte's virtual machine?
>
> A: No.
>
> Q: Mr. Leedom, where did you find the files that Mr. Schulte kept calling transcript files?
>
> A: They were all in unallocated space.
>
> Q: Did you draw any conclusions about what happened to those files from the fact that you found them in unallocated space?
>
> A: They'd been deleted.

(Tr. 1083). Only Schulte referred to this deleted data as a transcript file.

While forensic artifacts reflecting many of Schulte's actions on April 20, 2016 were nonetheless recovered by FBI experts from deleted space and from log files that Schulte failed to delete, not all of Schulte's actions were preserved. And that was precisely Schulte's intention. Among the files that Schulte deleted or destroyed are the files that would reflect precisely the commands that the Motion focuses on. Schulte's login to the Confluence virtual server would have been preserved in the Confluence virtual server itself. When Schulte attempted to log in to the Confluence virtual server on April 18, 2016, those login attempts were recorded in a log file stored in the Confluence VM itself. (GX1703-1 at 77, GX1207-26; Tr. 839-40). Schulte's log in to the Confluence VM on April 20, 2016, after he reverted to the April 16 snapshot, would similarly have been recorded in the log file, but that log file was destroyed when Schulte reverted back to the April 20 state without first taking another snapshot. Similarly, the commands Schulte entered to copy the Backup Files would have been logged within the Confluence VM, and those logs were similarly destroyed when Schulte reverted back to the April 20 snapshot. (Tr. 1084). Logs for device discovery, storage, and networking device and driver information are kept in the VM kernel log (GX1703-1 at 72, Tr. 876-77), which Schulte specifically deleted. (GX1703-1 at 71. 75, GX1203-29). Schulte specifically deleted the VM Ware log file (GX1703-1 at 83-84; Tr. 887-88), which records information about the operation of the Confluence virtual server, including device connections and data transfer logs (GX1703-1 at 84).

In sum, there was ample evidence from which the jury could reasonably conclude that the absence of log files reflecting Schulte's login to the Confluence virtual machine and his copying the Backup Files, including the destination where he copied those files, was the result of Schulte's destruction of evidence in order to cover his tracks.

There was sufficient evidence that the Backup Files were transferred during the April 20, 2016 Confluence reversion. Schulte argues that there was no testimony or evidence about DevLAN's network bandwidth or the copy speed of any external storage device used to receive the stolen Backup Files and, accordingly, no evidence from which the jury could infer that it was possible to copy the Backup Files during the time the Confluence virtual server was in its reverted state. (Mot. 54-57). Schulte's argument is specious and should be readily rejected.

The jury was certainly entitled to conclude from the facts that Schulte illegally accessed the Backup Files on April 20, 2016, and that data from those same files appeared on WikiLeaks beginning in March 2017 that Schulte copied those files on April 20. In other words, evidence that the Backup Files were copied is sufficient to show that it was possible to copy them, and Schulte's arguments to the contrary are sheer unfounded speculation. Schulte contends that the jury should have found that DevLAN had a particular network speed of 100 megabits per second and that, at this bandwidth, it would have taken longer than an hour and 20 minutes to copy the Backup Files. (Mot. 56-57). There was, however, no evidence that the network speed of DevLAN was so limited and, to the contrary, when asked about copy times at this hypothetical network speed, Mr. Leedom's response was, "Why would it only be 100 megabits?"[15] (Tr. 982). Indeed, the evidence showed that the Stash backups (the largest of the Backup Files) were typically both created and copied over the network to the Altabackup directory in approximately an hour and ten to an hour and fifteen minutes (*e.g.*, GX1207-47), far faster than Schulte's artificially slow scenario and a shorter time period than Schulte spent with the Confluence virtual server in its reverted states.

[15] For example, at 1,000 megabits per second, Schulte's own equation shows copying the Backup Files would lake less than ½ hour. (Mot. 56-57).

Similarly with respect to device copy speeds, Schulte fails to show that the jury could not have reasonably concluded that the Backup Files could have been copied to an external storage device. The jury could have concluded that there was time to do so on April 20, and also could have concluded that Schulte copied the Backup Files to another network location on DevLAN and then moved them to a storage device from there. (Tr. 976). The evidence amply demonstrates that the Backup Files were on April 20, 2016, and later transmitted to WikiLeaks, which is sufficient basis to conclude was possible to do so.

There is no support for Schulte's bathroom alibi. Schulte asserts that he was in the bathroom when the Backup Files were copied (Mot. 57-58)—essentially arguing no reasonable jury could have concluded that he was *not* in the bathroom. There is no evidence that Schulte was in the bathroom, and ample evidence that he was at his computer executing the commands reflected in the forensic evidence. CIA badge records simply show that Schulte's badge was used on one of the doors to the vault at 5:45 p.m., 5:48 p.m., and 6:48 p.m.,[16] before finally locking the vault at 7:07 p.m. (GX107 at 4). None of these conflict with the date-accessed time on the Confluence backup files (5:42 p.m. and 5:43 p.m.) or any of Schulte's other actions on DevLAN that evening.

There was sufficient evidence for the jury to conclude Schulte intended to regain his Atlassian administrator privileges by executing the Confluence reversion. Schulte argues that he could not have known that reverting the Confluence virtual server to the April 16 snapshot would restore his Atlassian administrator privileges because he "did not take the April 16, 2016

[16] There is no support for any part of Schulte's assertion (Mot. 57) that he tried to enter one vault door, found it locked, walked at a snail's pace down a short hallway to another vault door, re-entered the vault three minutes later, then continued walking at a snail's pace to his desk three minutes after that. The most reasonable inference is simply that Schulte checked the hallway to confirm no one would walk in on him while the files copied, but whatever his reason for opening the vault door, he was able to do so while copying the Backup Files.

snapshot." (Mot. 58-59). However, evidence shows that Schulte had administrator privileges on April 14, 2016, when he used them to restore his revoked project administrator status for OSB Libraries; Schulte knew he had no administrator privileges on April 18, 2016, when he was told that administrator had been transferred to ISB over the prior weekend (GX1064) and confirmed that his Confluence administrator logins no longer worked. (GX1703-1 at 31, GX1207-26). Schulte used his secretly retained OSB ESXi server root login to view the contents of the Confluence folder, which would have shown him the existence of the April 16, 2016 snapshot. (GX1703-1 at 39, GX1209-8). Schulte knew, with his experience as a former Atlassian administrator, that the snapshot likely was taken prior to changes to administrator privileges. (Tr. 742-43, 746, 1377-78). Schulte clearly expected his reversion to the April 16 snapshot to restore his administrator access to the Confluence virtual server and his access to the Altabackup directory, and the evidence was sufficient for the jury to so conclude.

There was no evidence that Schulte intentionally preserved a record of his activities on April 20, 2016. Similar to Schulte's false contention that a complete record of all of his actions on DevLAN on April 20, 2016 was preserved in a "transcript file," he also argues that his intentional creation of that file disproves any intention to unlawfully seal the Backup Files. (Mot. 59-60). As discussed above, *supra* 37-39, there was no evidence of a "transcript file" and Schulte intentionally destroyed copious amounts of data that would have recorded his actions on April 20, 2016.

There was sufficient evidence that the March 3, 2016 Backup Files were copied on April 20, 2016, during the Confluence reversion. In his final attack on the jury's verdict with respect to Count One, Schulte argues that there was insufficient evidence that the Backup Files were copied on April 20, 2016 because the "date modified" attribute of those files could have been affected by actions besides copying, and could have been intentionally changed at some other time by a "touch

command" (what Mr. Leedom described as "time stomping"). (Mot. 61-63). According to Schulte, the only evidence the Backup Files were copied on April 20, 2016 is this date-modified time, and that evidence does not "refute[] other possibilities," such as Schulte's fabricated scenario of a later break-in on DevLAN where the hacker noticed the April 20, 2016 date-modified information for the March 3, 2016 Backup Files and decided to steal those files to mask the date of the break-in.

Schulte's argument is legally, factually, and logically false. "[T]he government's case need not exclude every possible hypothesis of innocence," *Facen*, 812 F.3d at 286. The evidence need only support the jury's reasonable inference that Schulte stole the Backup Files on April 20, 2016. The date-modified attribute of the Confluence backups is far from the only evidence that he did so. *Supra* 5-21. The metadata on the March 3, 2016 Confluence backups showing they were copied on April 20, 2016, is consistent with and support the other evidence of Schulte's theft. Schulte's ability to devise implausible, speculative alternative explanations for the date-modified attribute does nothing to undermine the jury's reasonable verdict.

There was sufficient evidence of Schulte's transmission of the Backup Files to WikiLeaks. With respect to Count Two, Schulte argues that there was insufficient evidence for the jury to conclude that he transmitted the Backup Files to WikiLeaks because (1) there was insufficient evidence that he copied the Backup Files (incorporating his attacks on Count One), no data from the Backup Files and no evidence that he visited the WikiLeaks website in April or May 2016 was recovered from his home computers (Mot. 63-64); (2) there are innocent explanations for Schulte's downloading Tor and Tails and for wiping his hard drives (*id*. 65-67); (3) there was insufficient evidence of how Schulte transmitted the Backup Files to WikiLeaks (*id*. 67); and (4) "netflow logs" show that Schulte did not transmit the Backup Files using his home internet service. (*Id*. 68-70). Each of these arguments fails, for reasons that his similar attacks on Count One fail.

Just like his argument that the absence of particular forensic artifacts should have precluded the jury from finding that he copied the Backup Files, Schulte's argument about the absence of particular forensic artifacts of his transmitting the Backup Files fails. The trial evidence presented a compelling explanation for the absence of those artifacts: Schulte comprehensively destroyed that evidence by wiping his home computer and external hard drives and by using an anonymous web browser and an amnesiac operating system. *Supra* 18-19. Just as Schulte systematically attempted to delete log files that would reflect his theft of the Backup files, he took careful steps to destroy any forensic evidence of his transmitting those files, and the steps that Schulte took prevented the recovery of exactly the kinds of forensic evidence his Motion demands.

Schulte's attempts to offer speculative, factually unsupported explanations for his internet search history, Tor and Tails usage, and hard-drive wiping, fail. The trial evidence did not have to categorically exclude possible innocent explanations in order for the jury to reasonably find that Schulte transmitted the Backup Files, and in any event there is no evidence supporting Schulte's characterization of his "normal" home computer activity. The evidence at trial showed that Schulte repeatedly researched how to transfer large files and quickly calculate hash values, repeatedly researched secure data deletion and hard drive wiping, purchased a hard drive docking station that could connect external hard drives to his home computer, upgraded his Tor browser,[17] downloaded Tails, and then wiped his home computer, all during a short time surrounding his theft of the Backup Files and all consistent with Schulte transmitting the Backup Files to WikiLeaks and destroying evidence of having done so. *Supra* 18-19.

---

[17] Schulte asserts that the Tor browser was in a Linux VM that "Schulte never even used." (Mot. 65). Schulte repeatedly logged into that same Linux VM in the late night and early morning hours on April 30 and May 1, 2016. (GX1704-1 at 70-71, GX 1401-1, Tr. 1171-73).

Finally, Schulte argues that "netflow logs" prove that he did not transmit the Backup Files in April or May 2016. (Mot. 68-70). Reminiscent of Schulte's attempt to argue that the trial evidence included a "transcript file" recording every action he took on April 20, 2016, Schulte argues that DX208, a Verizon business record, is a "netflow log" recording all of his home internet data usage in April and May 2016. Once again, Schulte's argument finds no support in the trial record. There was no testimony that DX208 was a netflow log, no testimony explaining what DX208 did show or did not show, and no testimony supporting the conclusion that DX208 precludes the inference that Schulte transmitted the Backup Files. The only witness Schulte questioned about DX208, Mr. Berger, had not reviewed those records and was not familiar with what was included or was not included in them. (Tr. 1304). With no testimony about what DX208 reflects, what information it omits, or how to interpret that data, Schulte cannot rely on it to prove or disprove anything. In any event, as Schulte himself acknowledges, he had numerous means to transfer the Backup Files in addition to sending them to WikiLeaks from his home internet connection, including an alternative internet connection or public WiFi, an in-person meeting, or the mails. (Mot. 67). The evidence amply supports the inference that Schulte transmitted the Backup Files to WikiLeaks after stealing them, and DX208 falls far short of compelling the conclusion that Schulte could not have transferred the Backup Files.

In sum, there was ample evidence from which the jury could reasonably have found Schulte guilty of Counts One and Two.

2. Counts Five Through Eight: Computer Hacking and Computer Espionage in Connection With Stealing the Backup Files

Counts Five and Six charge Schulte with violating 18 U.S.C. § 1030(a)(1) and (a)(2) in connection with his unauthorized access to computers in order to steal classified information with reason to believe that information could be used to the injury of the United States or the advantage

of a foreign nation (Count Five) and to steal information from a United States agency (Count Six), in connection with his April 20, 2016 theft of the Backup Files from the CIA.

Counts Seven and Eight charge Schulte with violating 18 U.S.C. §°1030(a)(5) in connection with his transmission of harmful computer commands to a protected computer in connection with his manipulation of the state of the Confluence virtual server on April 20, 2016 (Count Seven) and his deletion of log files and other data (Count Eight).

As discussed above, on April 20, 2016, Schulte accessed multiple parts of the DevLAN network—a protected computer system for the exclusive use of the United States government—without authorization: he used his secretly retained SSH key access to open and use a root, or administrator, session on OSB's ESXi server despite no longer being a member of OSB and no longer having authority to act as an administrator on that server; he used his OSB server root access to revert the Confluence virtual server to restore his revoked Confluence administrator status and gain unauthorized access to the Confluence virtual server; and he used his unauthorized access to the Confluence virtual server to gain unauthorized access to the Altabackup directory. *Supra* 8-17. Schulte used those unauthorized accesses to steal the classified Backup Files from the CIA, which he had reason to believe could be used to the injury of the United States and the advantage of a foreign nation, and transmitted those Backup Files to WikiLeaks, and organization that Schulte knew was not entitled to receive them. *Supra* 18-19.

In the course of stealing the Backup Files, Schulte used his unauthorized access to execute numerous harmful computer commands that intentionally impaired the integrity and availability of data and information: he reverted the Confluence virtual server to the April 16, 2016 snapshot and, after approximately an hour and twenty minutes, reverted the Confluence VM back to an April 20, 2016 snapshot without saving the state of the VM, thereby erasing all records of his

actions inside the Confluence VM during the reversion period; and deleted the April 20, 2016 snapshot. *Supra* 16-17. Schulte also edited and deleted log files, rendering data available only through a forensic analysis of deleted file space and rendering some data unrecoverable. *Supra* 17.

Despite this evidence, Schulte argues that the jury could not reasonably have found him guilty of Counts Five, Six, Seven and Eight. With respect to Counts Five and Six, Schulte incorporates his arguments about the sufficiency of the evidence to show that he obtained and transmitted the Backup Files—evidence of access controls to the Altabackup directory, of his logging into the Confluence virtual server, of his copying the Backup Files, of his transmitting the Backup Files to WikiLeaks, (Mot. 71-74)—and those arguments fail with respect to Counts Five and Six for the same reasons that they fail with respect to Counts One and Two. In addition, Schulte also argues that (i) Count Five and Count Six are multiplicitous and the jury verdict violates the Double Jeopardy Clause of the Constitution (Mot. 73-74); (ii) there was insufficient evidence that Schulte used unauthorized access or exceeded his authorized access because on April 20, 2016, Schulte had authorized administrator access to the OSB server (25-28); (iii) there was insufficient evidence that Schulte used unauthorized access or exceeded his authorized access because Schulte's OSB server root access authorized any and all actions on the server (Mot. 28); (iv) Schulte's reversion and re-reversion of the Confluence virtual machine and his deletion of log files were authorized administrator actions and, indeed, "Schulte could have wiped the entire ESXi Server—and it would have been an authorized command" (Mot. 29-30, 32); (v) Schulte's reversion and re-reversion of the Confluence VM did not cause damage to DevLAN and he did not intend to cause damage to DevLAN because "reversions are typical administrator functions" (Mot. 30); (vi) the Confluence reversion, re-reversion, and snapshot deletion did not cause damage to DevLAN because re-reverting Confluence to the April 20, 2016 snapshot was necessary to

preserve the integrity of data on Confluence between April 16 and April 20 (Mot. 31); (vii) there was no damage caused by the reversion and re-reversion because "no data was lost" and "[t]here were no complaints from any users, and in fact, no one even noticed that the snapshot or reversion took place" (Mot. 31-32); (viii) the editing and deletion of log files did not cause any loss of data because "government experts could not say whether or not the log files were corrupted or contained any viable data" and "there was no activity that the logs would have captured that wasn't already recorded by the transcript files" (Mot. 33); and (ix) there was no evidence that the log files would have been preserved even if Schulte had not deleted them. (Mot. 33-34).

There was sufficient evidence that Schulte's access to OSB's ESXi server, the Confluence virtual server, and Altabackups was unauthorized. The Court has already denied Schulte's Rule 29 motion with respect to evidence of his unauthorized access to DevLAN (Tr. 1955-57), and the Motion provides no basis for reconsidering that ruling. Schulte's arguments about the scope of his authorization on DevLAN focuses solely on OSB's ESXi server and ignore the undisputed fact that on April 20, 2016, Schulte had neither administrator privileges nor administrator authority with respect to the Confluence virtual server or the Altabackup directory. Accordingly, regardless of Schulte's other arguments, his access to the Confluence VM and manipulation of and deletion of data from Confluence—including the deletion of the April 20, 2016 snapshot and the loss of unpreserved data from the period the VM was reverted to the April 16, 2016 state—and copying the Backup Files were unauthorized. *Supra* 16-17.

Moreover, the evidence clearly showed—and certainly is sufficient to support the jury's reasonable inference—that Schulte was not authorized to access OSB's EXSi server as an administrator or to perform any of the commands he executed on April 20, 2016. On March 31, 2016, Schulte was moved from OSB to RDB. (GX1046; Tr. 486-90, 1392). According to Mr.

Weber, after Schulte was moved to a different branch, he was no longer authorized to exercise administrator privileges on OSB's server. (Tr. 1601). On April 16, 2016, when Schulte's and other EDG developers' Atlassian administrator privileges were being removed, Mr. Weber also changed the password for the administrator login to the OSB server.[18] (GX1703-1 at 26-27, GX1209-12, GX1209-13, GX1209-15; Tr. 834-36, 1409).

Schulte's actions from April 15 onward reflect his own belief that, though he secretly maintained an SSH key login to OSB's server as an administrator, he was not in fact authorized to act as an administrator. On April 15, 2016, the day after he restored his OSB Libraries administrator status and before his Atlassian administrator status was revoked, Schulte logged in to the OSB server as "root" using his SSH key, and kept the session open. *Supra* 10. On April 18, 2016, after being told that his Atlassian administrator status was revoked, Schulte tested his administrator credentials to the Confluence virtual server (both username/password and SSH key) and also opened a second "root" session on the OSB server. *Supra* 13. Schulte then represented to Mr. Leonis that "I verified that all private keys with access have been destroyed/revoked" (GX1063), but said nothing about his SSH key access to the OSB server. On April 21, 2016, after breaking into the Altabackup directory and stealing the Backup Files, Schulte emailed Mr. Leonis about the OSB server, stating: "Not sure if this has been done already with my move to RDB, but I had equipment that was registered under my name for OSB… Notably, our $30,000+ server that I was custodian… Probably low on your totem pole, but what is the process for transferring this equipment to OSB and removing me from the CMR and my access." (GX1071). Schulte said

[18] As discussed above, though the administrator username/password access to the OSB server was changed, the SSH key accesses were not, apparently an oversight. *Supra* 11. Even if the SSH key accesses had been changed on April 16, 2016, it would have been too late, because Schulte already had opened a root session on April 15. *Supra* 10.

nothing about his administrator access to the OSB server, did not reveal that he still had a "root" session open on the server, and implied that Schulte believed that the server had already been re-registered and his accesses removed when Schulte moved to RDB.

Schulte could not help, however, boasting about his secretly retained administrator access to the OSB server, even with senior CIA leadership. During his June 30, 2016, meeting with then-Deputy Director of CCI Sean Roche, Schulte said, "I could restore my privileges if I wanted to, you know I could do that." (Tr. 1677).

From this evidence, the jury was permitted to infer that Schulte no longer had authority to access the OSB server as an administrator. Schulte argues that the jury was precluded from reaching this conclusion because (i) his April 18, 2016 email to Mr. Leonis about the revocation of his accesses had the subject line "ISB infrastructure permissions transfer" and, accordingly, addressed only the transfer of his Atlassian administrator privileges and did not misrepresent or misleadingly omit the status of his OSB server access; (ii) the "CMR" for the OSB Server was in Schulte's name, which was the equivalent of ownership or a "deed" to the server; (iii) Schulte's April 21, 2016 email to Mr. Leonis disclosed that the CMR for the OSB Server was still with Schulte and had the effect of informing Mr. Leonis that he still had administrator authority over the server, and Mr. Leonis implicitly assented to Schulte's continued OSB server administrator authority by failing to respond. (Mot. 25-27; *see also id*. 32). Schulte was free to argue this series of interpretations and inferences to the jury, but the jury likewise had sufficient evidentiary basis to reject them. Indeed, the evidence contradicts Schulte's assertions about the significance of the CMR: as Mr. Weber testified, CMRs were assigned to branches, and individuals were identified only as points of contact. (Tr. 1491-92). CMRs are an administrative mechanism for tracking property, and there was no testimony that CMRs had anything to do with administrator authorities

or privileges. (Tr. 621-23, 1491-92). The CMR did not, as Schulte claims, relate to administrator authority; even if it did, the CMR belonged to OSB, not to Schulte.

In sum, there was sufficient evidence for the jury to conclude that in April 2016, Schulte lacked administrator authority with respect to OSB's ESXi server.

There was sufficient evidence that Schulte was not authorized to access OSB's ESXi server, Confluence virtual server, and Altabackup directory as an administrator. Schulte argues that his manipulation of the state of the Confluence server and snapshot deletion on April 20, 2016 was not unauthorized because "[t]aking snapshots and reversions are typical administrative functions that are not inherently harmful like a computer virus or malicious action." (Mot. 30).

As described above, Schulte was not an authorized administrator on OSB's server, despite his secret root session, and his actions with respect to Confluence were not authorized. Moreover, there is no dispute that Schulte was not an administrator with respect to Confluence and was not authorized to revert the virtual server. OSB server administrator authorities would not extend to manipulating the Confluence VM—the OSB server administrator authorities extended to OSB virtual machines (Tr. 1376-77), but Confluence was not an OSB product, it was an EDG-wide resource with its own ISB administrators. The jury had sufficient evidence before it to reasonably conclude that Schulte's manipulation of the state of the Confluence VM was not authorized.

There was sufficient evidence that Schulte's manipulation of the Confluence virtual server impaired the integrity and availability of data and information. Schulte argues that his manipulation of the Confluence virtual server on April 20, 2016 did not cause damage because taking the April 20, 2016 snapshot and reverting back to that snapshot preserved the integrity and availability of data in the Confluence VM at the time the snapshot was taken and was "necessary for the integrity of the Confluence VM." (Mot. 31-32). Schulte's argument misses the mark.

"Damage" means "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. §º1030(e)(8). Schulte undeniably impaired the integrity and availability of information and data in the Confluence virtual machine when he re-reverted from the April 16, 2016, snapshot to the April 20, 2016, snapshot without saving any of the data or information from the prior state (including, specifically, data and information reflecting his actions in the Confluence VM during that time). *Supra* 16-17. The Motion does not address this destruction of data. Schulte also undeniably impaired the integrity and availability of the April 20, 2016, snapshot when he deleted it. Schulte argues that "no data was lost" because after the reversion back to the April 20, 2016, snapshot, the system resumed from that point. There was no evidence at trial, however, that a system resuming from a snapshot is the same as preserving the data in the snapshot itself, and the evidence in fact is to the contrary: the point of a snapshot is to preserve the state of the system at a point in time, because continued operation will change the data and make that state impossible to replicate without the snapshot.

There was ample evidence from which the jury could reasonably conclude that Schulte's manipulation of the Confluence virtual server on April 20, 2016, caused damage.

There was sufficient evidence that Schulte's editing and deleting log files on OSB's ESXi server was unauthorized or exceeded any authorization. For the same reasons that the jury had sufficient evidence from which it could reasonably conclude that Schulte was not authorized to access the OSB ESXi server in order to steal the Backup Files and manipulate the Confluence virtual server, it could reasonably conclude that he did not have authorization to access the OSB ESXi server as an administrator in connection with editing and deleting log files. (Mot. 32).

There was sufficient evidence that Schulte's editing and deleting log files impaired the integrity and availability of data and information. Schulte argues that editing and deleting log files

did not cause damage to DevLAN because (i) "government experts could not say whether or not the log files were corrupted or contained any viable data," (ii) "there was no activity that the logs would have captured that wasn't already recorded by the transcript files," and (iii) the deleted log files "certainly would have been deleted long before the WikiLeaks disclosure on March 7, 2017—so they would not have been available for the forensic experts in any case." (Mot. 32-33).

Schulte's first argument assumes that his deletion of the log files could not have impaired their availability or integrity if they were corrupted, and relies on testimony that does not support the assertion in any event. Schulte cites testimony by Mr. Leedom in response to cross-examination about vSphere. (Mot. 33; *see* Tr. 1073). vSphere is a local program that gives users access to the virtual server and the VMs running on it. (Tr. 743-44). The cited testimony simply is not about whether the log files on the OSB server that Schulte deleted were corrupted. Even if, hypothetically, some data in the log files were corrupted, Schulte impaired the integrity and availability of the files by deleting them. Schulte's second argument relies on the same mischaracterization about deleted file data (what Schulte insistently calls a "transcript file") that he relied on in seeking to overturn the jury's verdict with respect to Counts One and Two. *Supra* 37-39. Finally, with respect to Schulte's third argument, even if he were correct that log files might have been deleted in the ordinary course at some point, his deletions during the theft impaired their integrity and availability without authorization at the time of the deletion. Schulte is wrong in any event—the shell.log file, for example, still existed when the FBI conducted its forensic review (*see* GX 1703-1 at 37-39, GX1209-8), and incriminating evidence was recovered from its file slack.

In sum, there was ample evidence from which the jury could reasonably have found Schulte guilty of Counts Five, Six, Seven, and Eight.

Counts Five and Six are not multiplicitous. Schulte argues that Counts Five and Six are multiplicitous because classified information under § 1030(a)(1) is always information from a department or agency of the United States under § 1030(a)(2) and, accordingly, proof of one offense is always proof of the other. (Mot. 73-74). Schulte's analysis is incorrect.

To prove an offense under § 1030(a)(1), the government must prove that (i) the information at issue "has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data;" (ii) the defendant "reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation; and (iii) the defendant willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, or attempted to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the information to a person not entitled to receive it. § 1030(a)(1). To prove an offense under § 1030(a)(2), the government need only prove that the defendant obtained "information from any department or agency of the United States." § 1030(a)(2). Conversely, § 1030(a)(2) requires that the information be obtained "from" a U.S. department or agency, while § 1030(a)(1) requires that the information be classified, which can be information "owned by," "under the control of," *or* "produced by or for" the United States government. Exec. Order 13526 § 1.1(2) (Dec. 29, 2009). 75 Fed. Reg. 707 (Jan. 5, 2010). Thus, each offense requires proof of elements that the other does not, *see United States v. Garavito-Garcia*, 827 F.3d 242, 250 (2d Cir. 2016), and the counts are not multiplicitous.

3. Counts Three and Four: Transmission and Attempted Transmission of NDI from the MCC

Count Three charges Schulte with violating 18 U.S.C. § 793(e) in connection with his unauthorized possession and transmission of documents, writings, or notes containing NDI related

to the internal computer networks of the CIA transmission of in or about September 2018, while he was at the MCC. Count Four charges Schulte with violating 18 U.S.C. § 793(e) in connection with his unauthorized possession and attempted transmission of documents, writings, and notes containing NDI related to tradecraft techniques, operations, and intelligence-gathering tools used by the CIA between July and September 2018. § 793(e) makes it a crime to willfully communicate, deliver or transmit, or caused to be communicated, delivered or transmitted, documents, writings, or notes containing information pertaining to the national defense that the defendant had unauthorized possession of, to a person not entitled to receive it.

As discussed above, after Schulte was detained at the MCC pending trial, he obtained access to contraband cellphones that he used to begin executing what he called an "information war." Schulte documented his planned campaign in handwritten journals, where he also kept notes about passwords to encrypted and pseudonymous email and social media accounts, notes about concealing and deleting evidence, and draft social media postings revealing classified information. Schulte pretending to be a third person, sent a search warrant affidavit that was subject to a protective order along with Schulte's notes on the allegations, which contained classified information, to a reporter. He also opened a Buffer account to release social media posts and predetermined schedule and linked a pseudonymous Twitter account to it for the purpose of releasing his draft posts. *Supra* 26.

In his Motion, Schulte argues that the evidence was insufficient for the jury to find him guilty of Count Three and Four because (i) the information in the document that he transmitted to the reporter, and the information in the documents he drafted for release on social media concerning tradecraft and a particular CIA cyber tool, were not NDI (Mot. 4-9, 17, 19-24); (ii) Schulte lawfully possessed the documents and writings that contained NDO (Mot. 11-13, 15);

(iii) the materials that Schulte transmitted and attempted to transmit consisted of information, rather than documents, writings, and notes, which required proof under §°793(e) that Schulte had reason to believe the information could be used to the injury of the United States or to the advantage of any foreign nation (and the jury was required to be so instructed) (Mot. 11-13, 15-16); (iv) there was insufficient evidence that Schulte's transmission of NDI to the reporter was willful (Mot. 8-10); and (v) there was insufficient evidence that Schulte intended to transmit or attempted to transmit the NDI that is the subject of Count Four (Mot. 17-19, 21-22).

a. Schulte Transmitted and Attempted to Transmit NDI

NDI is information that it is directly and reasonably connected with the national defense, a broad term that refers to United States military establishments, intelligence, and to all related activities of national preparedness. The Government must also show that information related to the national defense is closely held by the United States government. *United States v. Abu-Jihaad*, 600 F. Supp. 2d 362, 386 (D. Conn. 2009); *see also Wilson v. CIA*, 586 F.3d 171, 174 (2d Cir. 2009); *United States v. Squillacote*, 221 F.3d 542, 575 (4th Cir. 2000).

Schulte argues that the information contained in the documents, writings, and notes he is charged with transmitting and attempting to transmit for various reasons does not relate to the national defense and that that the information is not NDI because it was not closely held or was already in the public domain.

The NDI in documents Schulte transmitted and attempted to transmit. In his September 24, 2018, email to the reporter, Schulte wrote, among other things, that:

> In reality, two groups—EDG and COG and at least 400 people had access. They dont [sic] include COG who was connected to our DEVLAN through HICOC, an intermediary network that connected both COG and EDG.

(GX812 at 3). At the time of the email, the number of people employed by EDG and COG was non-public. The fact that an unnamed group at CIA (EDG) with less than 200 employees had

access to DevLAN in March 2016 had been declassified specifically to include in a sealed, non-public search warrant affidavit that was provided to Schulte subject to a protective order restricting further disclosure. (Tr. 298-99, 430, 431-33, 1850; *see also* GX828).

At trial, multiple witnesses testified how information about the number of personnel assigned to particular CIA groups and about network infrastructure would be valuable to adversaries of the United States. Mr. Weber testified that information about the number of people in the CIA's COG group would be useful information to adversaries, and so would information about how COG and EDG were network connected. (Tr. 1593). Mr, Roche testified that the number of personnel assigned to particular groups or missions is classified because "it's an indicator of how much emphasis we're putting on a particular mission. The number will often have components that are in the foreign field, which can indicate who in the foreign field might be associated with a particular mission." (Tr. 1670-71). Mr. Roche elaborated that an adversary "can take a mosaic of information with that piece and then start working backwards to say for what this number is, where do we think these people are? What do we think activities we are seeing associated with this kind of mission? What do we think this group does specifically? How can we target those individuals if we get some bit of information or understanding that someone has a connection with this group?" (Tr. 1671).

In Schulte's draft social media postings, he wrote in the voice of a fictional CIA colleague who painted Schulte as a whistle-blower and scapegoat of the WikiLeaks investigation. In order to "authenticate" this fictional CIA officer, Schulte included classified information about CIA operations and cyber tools and revealed the true names of covert CIA officers. (GX809 at 8-13). Schulte wrote several variations of disclosures about a particular CIA cyber tool called "Bartender," which Schulte worked on during his CIA employment. (GX 809 at 8, 10, 11; Tr.

1421). In these draft social media postings, Schulte repeatedly identified Bartender as a piece of malware that had been "captured in the wild" and described in a cybersecurity vendor report, but whose connection to the CIA had not been discovered. Schulte wrote:

- "[Tool from vendor report] – Bartender for [redacted] [vendor]" (GX809 at 8)
- "Just to authenticate me first. The ~~@CIA~~ @USG was involved in [redacted] the code for the initially-planned cyber operation is in Vault 7. Additionally, [tool described in vendor report] is in fact Bartender. A CIA toolset for [operators] to [struck out] [redacted] configure for deployment" (GX809 at 10)
- "[@vendor] discussed [tool] in 2016, which is really the CIA's Bartender tool suite. [redacted]. Bartender was written [redacted] to deploy against various targets. The source code is available in the Vault 7 release." (GX809 at 11)

CIA officers testified about the harm to national security from providing details about Bartender's capabilities and publicly associating the CIA with malware that had been discussed in an industry publication. Mr. Weber described how identifying the known malware as a CIA tool would make it easier for other vendors to catch instances where the tool had been used, revealing CIA cyber operations and cyber targets. (Tr. 1422). Identifying the publicly known malware as a CIA tool would also increase the risk that other CIA tools with similar characteristics could be identified as being related to CIA cyber operations. (Tr. 1425). Identifying instances in which CIA tools had been deployed, in turn, would raise the risk that human assets who had assisted in its deployment would be identified and that they would face retribution, including (Tr. 1423), including execution. (Tr. 1366-67). This attribution risk was one of the biggest risks that Schulte and other AED developers concerned themselves with, and frequently discussed that risk and sought to mitigate it when designing cyber tools. (Tr. 1424-25; *see also* Tr. 1623).

Schulte also wrote a series of essays that he called his "articles," setting forth his narrative about his time at the CIA and his criminal prosecution and largely consisting of attacks against the government and the criminal justice system. Schulte posted nine of these articles on using a

WordPress account, which he linked from a Facebook account called "Who is John Galt?," named after the main character of Ayn Rand's novel, *Atlas Shrugged*. (GX824, GX825, GX826, GX830; *see also* GX809 at 3). The tenth article, which Schulte titled *Malware of the Mind* (*see* GX801, GX809 at 8), was addressed to "my fellow engineers and the tech industry" (GX801 at 2) and included the passage:

> Do you know what my specialty was at the CIA? Do you know what I did for fun? Data hiding and crypto. I designed and wrote software to conceal data in a custom-designed filesystem contained within the drive slackspace or hidden partitions. I disguised data. I split data across files and filesystems to conceal the crypto – how better to fool bafoons like forensic examiners and the FBI than to have custom software that doesn't fit into their 2-week class where they become forensic "experts". Make no mistake, I am an expert in data hiding and cryptography with thousands of hours of experience and among the top specialists in the world (or was).

(GX801 at 3). Schulte's notebooks similarly had notes on his intended disclosures of CIA cyber tool development techniques: "Small files are retained in FILE record whereas large files are stored in MSFT's dataruns. If you need help ask WikiLeaks for my code. I developed software to parse MSFT - NTFS & ext3 partitions so that I – for a [operation]."[19] (GX806 at 2). Mr. Weber testified that these types of disclosures raise attribution concerns. "The more hints and evidence that you give to the security community, the better posed they are to be able to detect your capabilities as well as potentially attribute it to a certain actor's activity." (Tr. 1417). Associating these techniques with particular operations raisees similar attribution risks. (Tr. 1417-18).

The evidence was sufficient for the jury to conclude the September 24, 2018 email contains NDI. Schulte argues that the September 24, 2018 email does not contain NDI because (i) information about Hickock was disclosed in WikiLeaks' Vault 7 release (Mot. 5-6); (ii) DevLAN

[19] MSFT refers to Microsoft, NTFS is a Windows files system, and EXT 3 is a Linux file system. (Tr. 1416-17).

and Hickock was shut down after the Vault 7 release and information about it "could not possibly compromise any CIA network or national defense" (Mot. 6-7); (iii) the information about Hickock was too generic to create a danger to national security and adversary intelligence agencies could not access DevLAN anyway because it was a closed network (Mot. 7); (iv) the Government did not call a classification expert (Mot. 7-8); (v) the CIA Hickock user guide was unclassified (Mot. 8); (vi) there was no evidence that Schulte was ever briefed on the number of COG personnel or that he actually knew how many personnel were assigned to COG (Mot. 8-9); and (vii) there was insufficient evidence that Schulte's transmission of information about Hickock and COG was the willful disclosure of NDI because his intent in sending the email to the reporter was to comment on search warrant affidavits that were unclassified. (Mot. 9-10).

Each of Schulte's arguments fails. The fact that CIA witnesses testified that disclosure of the information about Hickock and COG personnel would compromise national security and aid the United States' adversaries, and the reasons why the disclosure would have those effects, provides sufficient basis for the jury to reasonably conclude that the information relates to the national defense. In contrast, there was no testimony supporting Schulte's arguments that the information was too generic or too widely understood to qualify as closely held.

Schulte's contention that information about Hickock already was publicly disclosed does not preclude the jury from being able to reasonable conclude that the information about Hickock remained closely held. Schulte relies on information contained in Vault 7 (GX3009). As the evidence shows, the disclosed information was classified as Top Secret, and witnesses testified that (a) the CIA continued to treat information in Vault 7 as classified and subject to the associated handling and dissemination controls notwithstanding the WikiLeaks disclosure, and (b) at the time of Schulte's disclosure, the Government had not publicly confirmed the authenticity of any

information in WikiLeaks. (Tr. 298-99, 430-34, 1367-68, 1594-95). This was sufficient for the jury to reasonably conclude that the information in GX3009 remained closely held and NDI. *See Squillacote*, 221 F.3d at 577-79; *Fitzgibbon v. CIA*, 911 F.2d 755, 766 (D.C. Cir. 1990); *cf. United States v. Husayn*, --- U.S. ----, 142 S. Ct. 959, 968 (2022) ("information that has entered the public domain may nonetheless fall within the scope of the state secrets privilege"). Schulte's reliance on the unclassified version of the Hickock user guide fails for similar reason—the Hickock user guide was part of a leak that the government had not acknowledged—and an additional one: nothing in the user guide contains the information that Schulte disclosed to the reporter. (GX616). Schulte's Motion does not even attempt to identify any page of the User Guide that discloses the information contained in Schulte's email to the reporter.

Schulte's arguments that his disclosure about Hickock could not have harmed national security because DevLAN had been shut down as part of the investigation of the WikiLeaks releases, or because it was too generic to disclose useful information to an adversary, or because the information would be useless to adversaries because DevLAN was a closed system—an ironic argument from a cyber tool developer who specifically targeted closed networks—similarly fail to show the jury's verdict was unreasonable. Schulte fails to cite any evidentiary support for his arguments: the only testimony at trial was that the information contained in Schulte's disclosures would, in fact, aid adversaries. The jury could reasonably infer that information about how CCI's networks were constructed in the past would assist an adversary in analyzing historical intelligence, or in predicting the network architecture of future networks, or in drawing inferences about the relationship between the groups that used the network architecture. In any event, Schulte was free to argue his conclusions to the jury, but the jury was not required to accept them.

Schulte's final arguments with respect to Count Three require little additional discussion. The Government was not required to prove its case with particular forms of proof, *Persico*, 645 F.3d at 105 (sufficiency review is the same for direct and circumstantial evidence), and thus was not required call a classification expert (Mot. 7-8) or prove that Schulte was "ever briefed on the number of personnel in COG." (Mot. 9). *See also United States v. Lee*, 660 Fed. App'x 8, 15 (2d Cir 2016) ("No particular type of evidence is required," so long as the evidence taken as a whole is sufficient to support the verdict.). COG was EDG's "main mission partner" (Tr. 1381) and a typical "customer" for cyber tools developed by EDG (Tr. 650-51, 654) and Schulte certainly represented to the reporter that he knew the number of COG employees (GX812), which are sufficient to support the jury's verdict. Similarly, evidence that Schulte's motive for disclosing NDI to the reporter (Mot. 9-10) was to attack the investigation does not contradict the sufficiency of the evidence to show that, in doing so, he willfully disclosed NDI it to a person not authorized to receive it, particularly in light of ample evidence that Schulte intended to disclose NDI as part of his "information war." *Infra* 63-65. Finally, Judge Crotty's finding that evidence at a prior trial was insufficient to find that Schulte's disclosure about Hickock was NDI (Mot. 14 (citing D.E. 581 at 25)) is not binding where here there was, among other things, testimony that the disclosure of information about how EDG and COG were network-connected would be useful to adversaries and documentary evidence that the network architecture was Top Secret information. (GX3009; Tr. 1593). *Cf.* D.E. 650 at 4; Dec. 12, 2021 Tr. at 70 (denying motion to dismiss Count Three).

The evidence was sufficient for the jury to conclude Schulte attempted to disclose NDI. Schulte argues that the evidence was insufficient to support a reasonable finding that he attempted to disclose NDI as charged in Count Four because (i) there was no transmittal of Malware of the Mind except to Schulte's attorneys and no evidence of an intention or attempt to transmit Malware

of the Mind (Mot. 17-19); (ii) the information about cyber tool techniques in Malware of the Mind is too generic to be NDI (Mot. 17); (iii) Schulte intended to rewrite Malware of the Mind and could have removed the NDI from the final draft (Mot. 19); (iv) information about Bartender was not NDI because it was "shut down" and it was exposed in the WikiLeaks leaks (Mot. 19-20); (v) information about Bartender was not NDI because the information was too generic and tool names are not classified (Mot. 20-21); (vi) there was no evidence that Schulte attempted to transmit the draft posts about Bartender (Mot. 21-22); (vii) the fact that the Government declassified certain information in connection with this prosecution proves its disclosure could not cause harm (Mot. 22-23); and (viii) there was no evidence Schulte intended to willfully transmit NDI because he "knows real national defense information" and "[i]f and when Mr. Schulte ever decides to wage a war against the United States, he could easily cause true catastrophic damage." (Mot. 23-24).

There was ample evidence from which the jury could reasonably conclude that Schulte intended to publish the Bartender posts and Malware of the Mind, and took substantial steps towards doing so. As described above, between July and September 2018, Schulte engaged in an "information war" to attempt to influence public opinion about his case and to retaliate against the government for prosecuting him. Schulte repeatedly wrote about his desire to harm the United States government by disclosing classified information about drafted social media postings and articles exhorting others to do the same (*e.g.*, GX 809 at 2 ("I will look to breakup diplomatic relationships, close embassies, end U.S. occupation across the world & finally reverse U.S. jingoism. If this is the way the U.S. govt treats one of their own, how do you think they treat allies?"), 11 (#Top Secret #FuckYourTopSecret --> or dump the secrets here:"), ; 12 ("To the United States Intelligence Community – why would you keep ~~America's~~ the govt's secrets when ~~your own country~~ the govt wrongly prosecutes your own?"), 13 ("Until your ~~country~~ govt protects

you and honors your service, send all your govt's secrets here: WikiLeaks"), & 15 ("Monday 17th - Tues 18th – DL Disc, UL WL"); GX820-430 & -431 ("Essentially, it's the same thing as taking a soldier I the military, handing him a rifle, and then begin beating him senseless to test his loyalty and see if you end up getting shot in the foot or not. It just isn't smart."); and hiding and deleting evidence of his scheme. (GX809 at 5, 7 ("Yesterday I started cleaning the phone….")).

In addition to powerful evidence of Schulte's intention to disclose classified information generally, Schulte took substantial steps towards publishing the Bartender posts and Malware of the Mind. Schulte wrote several drafts of the Bartender tweets (along with others), growing more detailed and specific with each draft. (GX809 at 8, 9, 10). He created Wordpress, Twitter, Facebook, and Buffer accounts using his contraband cellphone, and linked the Facebook account to the Buffer account. (GX809 at 5-6, 14-16, GX823-826, GX830, GX1302-1, GX1303-44 -1303-64, DX815). He wrote 10 articles, of which Malware of the Mind was tenth (GX809 at 3, 7, 8) and in late September 2018 began posting the first nine articles while he rewrote the tenth. (GX809 at 16, GX1303-68, GX825, GX826, GX830).[20] In mid-September, Schulte was writing out a schedule of public releases, including tweets and transmissions to WikiLeaks. (GX809 at 15). As Carlos Betances, an inmate who helped Schulte and others get access to contraband cellphones, testified, Schulte was trying to smuggle a USB drive into the prison (Tr. 1756) and, when Betances prevented him from doing so, attempted to smuggle one of the contraband cellphones into the prison law library to "send something very important." (Tr. 1754-55). Schulte's efforts to publish

[20] Earlier in 2018, Schulte's parents posted prior drafts of his articles to a Facebook page. (GX806 at 3). In September, Schulte created a new Facebook page and Wordpress account to upload his articles himself. *Supra* 25-26, 64.

additional materials were disrupted on October 3, 2018, when the FBI executed a search warrant at the MCC and seized the contraband phones and Schulte's notebooks. (Tr. 1813-14, 1819-20).

This evidence of Schulte's desire to publicly release classified information, his actual publication of several of his "articles" while he revised his draft tweets and tenth article, his creation of various social media accounts in order to be able to publish his writings, the fact that his draft tweets and Malware of the Mind are explicitly addressed to a public audience, and Schulte's linking of the @freejasonbourne Twitter account to his Buffer account are more than sufficient basis for the jury to reasonably conclude that he intended to publish the Bartender Tweets and Malware of the Mind, and that he took very substantial steps in furtherance of that goal. There is no evidence supporting Schulte's assertion that he intended to remove NDI from Malware of the Mind (Mot. 19), and evidence that he provided a draft to his attorneys (Mot. 17-19) is not inconsistent with his intent to publish the article on the internet.

As described above, CIA officers who are experts in cyber operations testified about the harm to national security from disclosing the information about Bartender in Schulte's proposed tweets and cyber tool development in Malware of the Mind. *Supra* 58-59. That testimony was sufficient for the jury to reasonably conclude that the information in the draft writings was NDI, and Schulte's arguments to the contrary are unavailing. There was no testimony supporting Schulte's arguments that the information in Malware of the Mind and the Bartender tweets was "too generic" to be NDI. (Mot. 17, 20-21). With respect to Bartender, Schulte mischaracterizes the relevant NDI in any event; whether tool names are, standing alone, considered unclassified, the undisputed testimony was that associating a tool name with the tool's functionality is classified, and certainly that disclosing that a publicly identified piece of malware is associated with the CIA creates grave risks to cyber operations and CIA assets. *Supra* 58. Those risks to assets and past

operations, and the risk that attributing one cyber tool to the CIA past operations and assets increases the likelihood that other cyber tools (and other operations and assets) will also be exposed is not diminished by the disruption in Bartender's development caused by the Vault 7 release. (Mot. 19-20). The attribution Schulte intended to make between Bartender and the malware described in the vendor report was not disclosed in the WikiLeaks leaks. (Tr. 1604-05). Finally, the fact that some formerly classified information was declassified for use in connection with the investigation and prosecution of Schulte (Mot. 22-23) has no bearing on whether the information was NDI at the time of Schulte's transmissions and attempted transmission, particularly where NDI can be declassified for reasons of public interest. *See* 32 C.F.R. § 2001.35.

The evidence described above is replete with indications of Schulte's intent to willfully disclose NDI, and the fact that he knows other NDI that was not included in the Bartender tweets and Malware of the Mind, but which he continues to threaten to potentially disclose at some point in the future (Mot. 23-24), does not undermine the jury's determination that those attempted transmissions were willful.

b. The Indictment was not constructively amended.

Schulte also argues the Indictment was constructively amended because Count Three alleges, in a "to wit" clause, that Schulte violated Section 793(e) by transmitting documents, writings, and notes pertaining to internal computer networks of the CIA; but the proof at trial included his transmission of documents, writings, and notes pertaining the number of personnel assigned to COG, a user of that computer network. (Mot. 8-9). The Second Circuit, however, has "never suggested that a 'to wit' clause binds the government to prove the exact facts specified in a criminal indictment." *United States v. Bastian*, 770 F.3d 212, 221 (2d Cir. 2014) (rejecting claim that proof of a different firearm than that alleged in the indictment was a constructive amendment of a § 924(c) count); *see also United States v. D'Amelio*, 683 F.3d 412, 422 (2d Cir. 2012) ("The

essential element at issue is [the defendant's] use of a 'facility or means of interstate . . . commerce,' 18 U.S.C. § 2422(b), not the particular means that were used."). That the proof at trial showed that Schulte violated § 793(e) in ways additional to that identified in Count Three's "to wit" clause is not a constructive amendment.

c. The MCC Counts do not violate the First Amendment.

Schulte argues that the MCC Counts are vindictive. (Mot. 24).

> [T]he decision as to whether to prosecute generally rests within the broad discretion of the prosecutor, and a prosecutor's pretrial charging decision is presumed legitimate. However, to punish a person because he has done what the law plainly allows him to do is a due process violation of the most basic sort, and a prosecution brought with vindictive motive, penalizing those who choose to exercise constitutional rights, would be patently unconstitutional. Accordingly, an indictment will be dismissed if there is a finding of actual vindictiveness, or if there is a presumption of vindictiveness that has not been rebutted by objective evidence justifying the prosecutor's action.

United States v. Sanders, 211 F.3d 711, 716 (2d Cir. 2000) (cleaned up).

Schulte has not pointed to any circumstances showing that Counts Three and Four were filed as "a direct and unjustifiable penalty that resulted solely from the defendant's exercise of a protected legal right," *id*. at 716-17 (cleaned up), that is, prosecutorial animus toward the defendant, *id.* at 717; or "that the circumstances of a case pose a realistic likelihood of such vindictiveness." *Id*. (cleaned up).

d. The documents, writings, and notes at issue were not lawfully possessed

Schulte argues that he lawfully possessed intangible information (Mot. 11, 13) and "[a]nything Schulte writes is lawfully possessed by him." (Mot. 14). The writings containing NDI that Schulte possessed at the MCC were not lawfully possessed. As the evidence at trial showed, classified information is subject to handling requirements. (Tr. 120-21, 225, 459-64, 1595-96). A basic handling requirement is that classified information cannot be taken outside of the CIA

without a security review and approval. (*Id*.). Schulte was aware of this requirement, as demonstrated by his false denial of having retained a copy of the email he sent on his final day at the CIA, which contained classified information. *Supra* 23. Schulte cannot create classified documents, writings, and notes that violate the handling requirements for classified records, and his possession of those materials at the MCC was unlawful.

e. Schulte was properly charged under the "information" prong of § 793(e)

Schulte argues that he should have been charged under the "information" prong of Section 793(e) or, in the alternative, under the "lawfully possessed information" prong of Section 793(d), rather than the "documents, writings, and notes" prong of Section 793(e), in Counts Two, Three, and Four. (Mot. 11-14 & 15-17). Schulte argues that the material he is alleged to have transmitted and attempted to transmit consists of intangible information, regardless of whether it was committed to a writing or a document and that he was lawfully entitled to possess the intangible NDI that he learned while employed at the CIA.

Schulte's interpretation of § 793 would read the "documents, writings, and notes" prong of the statute out of existence. Documents, writings, and notes only "relat[e] to the national defense" to the extent that there is information about them or contained within them that constitutes NDI. If only the information prong of the statute were available when the defendant transmits otherwise-intangible NDI that has been committed to a writing, the "documents, writings, and notes" prong could never be invoked. Moreover, the law is clear that "[w]hether to prosecute and what charge to file or bring before a grand jury are decisions that generally rest in the prosecutor's discretion." *United States v. Batcheler*, 442 U.S. 114, 124 (1979). "[A] defendant has no constitutional right to elect which of two applicable federal statutes shall be the basis of his indictment and prosecution." *Id.* at 125. That discretion cannot be exercised for unconstitutional reasons, *id*. at 124-25 & n.9,

but it encompasses which sentencing scheme should be invoked, *id*. at125, or which elements must be proved. Here, there is no doubt that the attachment to the September 24, 2018 email was a "document, writing, or note," nor any doubt that the social media posts Schulte intended to make were "documents, writings, or notes." *Cf. Bazak Int'l v. Tarrant Apparel Group*, 378 F. Supp.2d 377, 383 (S.D.N.Y. 2005) (intangible messages like emails are writings under the Uniform Commercial Code). The conduct was properly charged.

4. Count Nine: Obstructing a Grand Jury Proceeding

Count Nine charges Schulte with violating 18 U.S.C. § 1503 resulting from false statements that he made to the FBI from in or about March 2017 to June 2017. § 1503 makes it a crime to knowingly and corruptly obstruct or impede, or attempt to obstruct or impede, a proceeding pending before a grand jury. As described above, Schulte was interviewed by the FBI on March 14, 2017, and served with two grand jury subpoenas. One subpoena required him to testify before the grand jury on March 17, 2017. After being served with the subpoenas, Schulte falsely claimed his diplomatic passport was at his apartment and falsely denied having classified records at his apartment. Later that night, Schulte retrieved his diplomatic passport from his office at Bloomberg. *Supra* 73. Rather than testify before the grand jury, Schulte was interviewed at the U.S. Attorney's office on March 20 and 21, 2017, with counsel, agents, and AUSAs present. Schulte falsely denied being involved in the WikiLeaks Disclosures, denied having made DevLAN vulnerable to compromise, offered ways in which classified information could have been stolen that Schulte knew were not the way that he had stolen the Backup Files, and directed the FBI toward log files that Schulte believed he had deleted. *Supra* 23-24.

Schulte argues that the evidence was insufficient for the jury to find him guilty because (i) "the government failed to establish what happened with [the] subpoena or whether the grand jury continued to operate into June of 2017" (Mot. 35); (ii) there was no evidence Schulte knew

what a grand jury was or that it would continue to convene after March 17, 2016 (*id.*); (iii) Schulte did not know his statements to the FBI would be presented to the grand jury (Mot. 36); and (iv) Schulte did not lie to the FBI. (Mot. 36-37).

In light of the facts that the two grand jury subpoenas were served on Schulte by FBI agents, and Schulte lied to these same FBI agents; that the grand jury subpoenas required Schulte's telephone to be presented to the grand jury and required his testimony on March 17, 2016; and that Schulte lied to the FBI after having received the subpoena on March 14, 20, and 21, 2016; the jury could reasonably conclude that Schulte both knew the grand jury proceeding was pending when he lied to the FBI and was aware that his statements to the FBI were likely to affect or influence the grand jury proceedings. Indeed, one clear inference from the evidence is that Schulte hoped his false statements would deflect suspicion away from himself, focus the investigation on unproductive avenues chasing incorrect theories of how the offense was committed, and avoid being called to provide testimony directly to the grand jury. This evidence was sufficient for the jury to reasonably conclude that Schulte knew the grand jury proceedings were pending and that his false statements were intended to corruptly obstruct and impede those proceedings. *See, e.g.*, *United States v. Sutherland*, 921 F.3d 421, 428 (4th Cir. 2019) (finding sufficient causal relationship under § 1512(c)(2) between defendant's submission of false documents to the U.S. Attorney's office and a pending grand jury proceeding); *United States v. Reich*, 479 F.3d 179, 185 (2d Cir. 2007) (finding sufficient nexus under § 1512(c)(2) between submission of forged court order to a party to a court proceeding and the party's dismissal of that proceeding).

There was also sufficient evidence for the jury to reasonably find that Schulte's statements to the FBI were intentionally false. The jury could reasonably find (and the evidence compellingly demonstrates) that Schulte was asked about the classified email and intentionally denied

possessing it, that Schulte stole the Backup Files and falsely denied having done so, that Schulte had compromised security on DevLAN by abusing his SSH key access to the OSB ESXi server to manipulate the Confluence VM and delete log files and falsely denied having done so; that Schulte knew he had deleted log files that would have shown his theft (and believed he had deleted all of them) and attempted to mislead the investigation by highlighting them, and that Schulte knew how he had committed the theft and proffered alternative means of committing the crime to deflect suspicion and divert the investigation.

II. Schulte's Motion for a New Trial Should Be Denied

In addition to his motion for a judgment of acquittal, Schulte seeks a new trial pursuant to Rule 33, arguing that he did not have a fair trial without the production of forensic images of the entire DevLAN network, including (i) "access to the ESXi Server Altabackup/FS01 Server, all networking devices connecting them, and any and all other servers and networking devices that the data could have been copied to" (Mot. 79, 83-84, 86-89), (ii) "broad access to every single seized DevLAN device" (*id*. 79), (iii) Schulte's CIA workstation (*id*. 80-84), (iv) access to all of Mr. Schulte's removable media and accountable property (id. 83), (v) "every single backup from March 3, 2016 to March 6, 2017" (*id*. 91), (vi) "access to the Stash and Confluence servers" (*id*. 91-95), (vii) source code for cyber tools including Brutal Kangaroo, Bartender, and Nader (*id*. 95-97), (viii) access to the offsite backups of the Atlassian products (id. 97-98), (ix) access to Jira and Hickock (*id*. 98-99), and (ix) "forensic images and discovery about the DevLAN-international connection." (*Id*. 100-01). Schulte also argues that the trial was unfair because the defense made requests for particular network or forensic data, which revealed defense strategy and led to the production of incriminating evidence. (*Id*. 102; *see* GX1207-27 & 1207-30). Finally, Schulte argues that he is personally entitled to access to this classified discovery, and that the requirements of a fair trial are not satisfied by providing access to classified discovery to defense counsel and

defense experts. (Mot. 106-107). In addition to arguments about DevLAN, Schulte also asserts he was denied a fair trial without access to an AFD report and personnel. (Mot. 108-09).

Finally, Schulte argues that the Government committed misconduct by making allegedly prejudicial statements during jury addresses. (Mot. 110-11).

A. Background

1. Prior Motions to Compel Additional Classified Discovery from DevLAN

On July 22, 2019, Judge Crotty entered an order pursuant to CIPA § 4, 18 U.S.C. App. A, directing the Government to provide certain discovery materials to defense counsel and otherwise granting the Government's motion to delete classified information from discovery. (D.E. 124). The Order was entered after *ex parte* conferences with both the Government and with defense counsel. *Id*. at 2. Judge Crotty noted that "Schulte has requested that the Government provide him with a complete forensic copy of the Schulte Workstation and DevLAN, so that his cleared expert can conduct a comprehensive forensic analysis to rebut the Government's forensic case and show that individuals other than Schulte within or outside the CIA could have or did steal the leaded data." (*Id*. at 11). The Government produced data and records from Schulte's workstation and from DevLAN according to a methodology designed to exclude irrelevant and/or classified information, to protect national security interests while also providing the defense access to relevant information, *id*.; and also committed to work with the defense and CIA to produce additional material "to the extent Schulte articulated a justifiable need" for it. *Id*.

"[M]indful of the immense size of the full universe of forensic data and of the serious national security concerns inherent to producing the totality of Schulte's requests," the Court noted the "great deal of planning and effort" the Government invested "in collecting, reviewing, and

producing what might be an unprecedented volume of classified discovery to Schulte."[21] *Id*. Particularly where Schulte was charged with leaking information he obtained from the CIA, "[g]ranting him unfettered access to the Schulte Workstation and DevLAN would gut the entire rationale of CIPA. There is clearly 'a reasonable danger that disclosure of this evidence will expose . . . matters which, in the interest of national security, should bot be divulged.'" *Id*. at 12 (quoting *United States v. Aref*, 533 F.3d 72, 80 (2d Cir. 2008)). Judge Crotty denied Schulte's request, leaving "open the possibility of ordering production of forensic data beyond what supports the Government's own theory of the case if Schulte submits a more tailored request and provides good reason for further forensic discovery in a motion to compel." *Id*.

Schulte filed motions relating to discovery from DevLAN on February 18, 2020 (D.E. 328), and July 28, 2020. (D.E. 420), and filed a *pro se* letter September 21, 2021 (D.E. 504), seeking the production of forensic images of the "forensic crime scene"—Schulte's CIA workstation, the NetApp (or FS01) server, and OSB's ESXi server. (*Id*. at 3-11). The Government opposed (D.E. 329 & 423), noting, among other things, that additional forensic discovery had been produced as outlined in the § 4 order. (D.E. 423 at 1-2).

Judge Crotty denied the motions. (D.E. 514). Schulte's new motions were "no more meaningfully tailored than Schulte's prior request for a full forensic copy of DEVLAN." *Id*. at 4.

> [Schulte] still articulates no specific rationale for why he should be entitled to mirror images of two entire servers containing troves of classified material with no relevance to this action whatsoever. The ESXi server contains data related to an array of classified programs with no relationship to Schulte's work at the CIA, much less the charges against him. Likewise, the NetApp server contains folders for individual employees' work product, final cyber tool products, and daily backups of DEVLAN's components, the vast majority of which are unrelated to

[21] The discovery included all log files from OSB's ESXi server, the relevant backups (*i.e.*, the March 3, 2016 Confluence backup files) from the NetApp server, and all portions of unallocated space for the ESXi server about which Mr. Leedom testified. (D.E. 423 at 1-2).

> this case. To be sure, the servers do also contain materials of significance to this case, and to that end, the parties have coordinated the disclosure of a substantial volume of classified and unclassified data.

Id.

On January 22, 2022, Schulte filed a *pro se* omnibus motion seeking, among other things, to preclude the Government's expert witnesses from testifying about DevLAN (D.E. 765 at 40-46) and to compel disclosure of complete copies of the stolen Backup Files and all other Confluence and Stash backup files. (*Id*. at 48-50). The Government opposed, noting that the defense expert had been provided access to complete copies of the March 2 and 3, 2016 Confluence databases, all Confluence data points used in Mr. Berger's timing analysis, complete copies of the Stash repositories for the tools for which source code had been released by WikiLeaks, complete copies of all Stash documentation released by WikiLeaks, and all commit logs for all projects released by WikiLeaks (redacting only the names of particular users). (D.E. 761 at 40-41). In reply, Schulte renewed his prior requests for complete copies of Schulte's workstation, the NetApp server, and OSB's ESXi server. (D.E. 793). The Court ordered additional briefing and expert declarations. (D.E. 767, 787, 791). The Government also provided the Court with copies of all classified discovery cover letters. (D.E. 795).

By order dated May 24, 2022, the Court denied Schulte's motions to preclude and to compel. (D.E. 823). The Court held that Schulte's interest in reciprocal discovery is limited by the Government's countervailing interest in maintaining the confidentiality of classified information. (*Id*. at 3). Having reviewed the history of classified discovery in the case and the parties' submissions, the Court was "not persuaded that Defendant lacks any information he would need to effectively cross-examine the Government's experts." (*Id*. at 4). The Court denied Schulte's motions to preclude and to compel, finding that "nearly all of the information he seeks has already been provided, and he has not shown how additional information would be 'helpful or material to

the defense.'" (*Id*. at 5 (quoting *Aref*, 533 F.3d at 80)). With respect to Schulte's renewed request for complete forensic images of DevLAN, "the Court [was] not persuaded that his arguments justify revisiting Judge Crotty's prior rulings on this issue. Defendant's expert speculates about exculpatory evidence he might find if given access to the full range of forensic discovery in the Government's possession, but he offers no reason to believe any of that evidence actually exists." (*Id*. at 7-8). The Court noted that the defense expert "raises a host of other issues which may be proper arguments at trial, but are not the subject of this motion to compel." (*Id*. at 8 n.4). At trial, Schulte did not call an expert witness.

2. Prior Motions to Compel AFD Discovery

Schulte has repeatedly claimed that a CIA group called AFD produced a "forensic examination and analysis" of DevLAN, based on a reference to information provided to the FBI by AFD. (D.E. 504 at 1, 11; D.E. 605 at 2-3; D.E. 644 at 6-7; D.E. 661 at 5). The Government has repeatedly confirmed that no such document exists. (D.E. 591 at 3-4; D.E. 647 at 2). Information responsive to defense requests, as well as information from a different CIA entity, the WikiLeaks Task Force, was provided to Schulte. (D.E. 591 at 3). The Court denied Schulte's motion to compel the non-existent AFD document. (Dec. 20, 2021 Tr. at 6-7).

B. Applicable Law

Federal Rule of Criminal Procedure 33 provides that "[u]pon the defendant's motion, the court may vacate any judgment and grant a new trial if the interest of justice so requires." Fed. R. Crim. P. 33(a). This discretion should be exercised "sparingly and in the most extraordinary circumstances, and only in order to avert a perceived miscarriage of justice." *United States v. Gramins*, 939 F.3d 429, 444 (2d Cir. 2019) (cleaned up). "[T]he 'ultimate test' for granting a new trial pursuant to [Rule 33] is 'whether letting a guilty verdict stand would be a manifest injustice.'" *Id*. (quoting *United States v. Ferguson*, 246 F.3d 129, 134 (2d Cir. 2001)). "There must be a real

concern that an innocent person may have been convicted." *United States v. Sanchez*, 969 F.2d 1409, 1414 (2d Cir. 1992).

C. Discussion

1. DevLAN Discovery

Schulte's arguments about forensic discovery revisit discovery that he repeatedly sought, and repeatedly was denied under CIPA: access to all of the classified data on DevLAN. Indeed, Schulte expands on his pre-trial requests to argue he was entitled to broader disclosure, including offsite backups, overseas network components, and to personal access to everything rather than access by defense counsel or experts. Concerningly, Schulte makes this same sweeping demand in the very same motion in which he threatens, "[i]f and when Mr. Schulte ever decides to wage a war against the united States, he could easily cause true catastrophic damage." (Mot. 23-24).

Schulte's Rule 33 motion fails to show that the Court's prior CIPA rulings resulted in a "manifest injustice" warranting a new trial. Indeed, Schulte fails to show that the Court's orders were error at all. Significant portions of Schulte's Rule 33 motion simply repeat his pretrial arguments and suffers from the same flaws: he fails to show any reasonable likelihood that access to that data would have been "material and helpful to the defense." (D.E. 823 at 3 & 7 (quoting *Aref*, 533 F.3d at 80)). For example, Schulte argues that he needed access to all of the Stash and Confluence backups in order to test Mr. Leedom and Mr. Berger's timing analyses, a repeat of his pretrial motions. (*Compare* Mot. 89-91 *with* D.E. 504 at 7-9, D.E. 644 at 10-11, and D.E. 765 at 48-50). Unlike his pretrial motion, Schulte does not even provide a factual basis for his argument in the form of an expert affidavit; he simply makes a series of broad and speculative assertions with no factual foundation. (D.E. 767 (ordering submission of expert affidavits in connection with motion to compel)).

To the extent Schulte makes new arguments about why access to additional data would have been helpful to the defense, he offers no excuse for failing to make those arguments prior to trial. Schulte, defense counsel, and the defense expert were repeatedly invited to make tailored requests for electronic discovery, and when they did so the Government worked to make the requested data available. (D.E. 124 at 10; *see also id.* at 12-13 & n.6 (noting that the Government and the defense have been cooperating to resolve discovery disputes, and the Government's expert had met with the defense expert); D.E. 329 at 9-10; D.E. 423 at 2). Prior to trial, Schulte had received copies of every piece of forensic data that the Government's experts relied on in conducting their analyses and reaching their conclusions, as well as their notes and other 3500 material, their testimony at the 2020 trial, and copies of the presentations the experts would use during their testimony. Schulte had ample basis and opportunity to make any tailored request for discovery he needed, and no excuse for failing to raise any such requests earlier.

Schulte's new arguments do not show manifest injustice or the likelihood that an innocent person was convicted. Schulte argues that he needed access to the entire DevLAN network in order to conduct a "bandwidth analysis" (Mot. 78-79) but does not explain what that analysis would have been, why access to the entirety of the classified information on DevLAN was needed, or show any realistic possibility that the results would have been helpful. Notably, the trial evidence did include bandwidth evidence, which showed that Confluence backups were copied from the Confluence virtual server to the Altabackup directory in a couple of minutes and Stash backups were copied from the Stash server to the Altabackup directory in approximately an hour-and-ten to an hour-and-fifteen minutes. (*E.g.*, GX1207-29, GX1207-47). Schulte also had the opportunity to cross-examine three other DevLAN users about network bandwidth.

Schulte asserts that he needed complete access to the entire DevLAN network to search for anywhere on the network that the Backup Files could have been staged in order to disprove they were used (Mot. 79-80), access to the entire NetApp server and Altabackup directory to "search for the proof that the altabackup directory was wide-open" and "search every single DevLAN device for forensic evidence that the altabackup directory contained no access controls" (Mot. 88), access to the entire Confluence and Stash servers to see if the March 3, 2016 backup files could have been automatically accessed as a result of the April 16, 2016 snapshot (Mot. 92), access to all offsite backups in order to determine if any one of them could have been the source of the WikiLeaks Disclosures (Mot. 97-98), access to a complete copy of the Jira and Hickock servers to see if COG users could access the Altabackup directory (Mot. 98-99), and access to all international network components to see if DevLAN could have been compromised by a foreign intelligence service. (Mot. 100-01). Schulte made none of these requests prior to trial, but even if he had, he fails to identify how any of that was necessary to test the analyses and conclusions that the Government experts *did* conduct. Schulte essentially argues that he has a "constitutional right to conduct his own search of the [Government's] files to argue relevance"—a right that he unequivocally does not have, *Pennsylvania v. Ritchie*, 480 U.S. 39, 59 (1987), especially where access to huge volumes of irrelevant classified information is at stake.

The motion is also littered with false descriptions of discovery, mischaracterizations of the evidence, and contradictions. For example,

- Schulte contends "the government presented literally zero logs from Mr. Schulte's CIA Workstation to the jury." (Mot. 81). To the contrary, viclient logs from Schulte's workstation were introduced and were the subject of expert testimony. (GX1703-1 at 12, 13, 49, 51, 54-55, 61, 63, 64; GX1202-7, -8, -16, -17, -18, -19, -20, -21).

- Schulte argues that his "virtual machine was only 50 GB in size," but in the very next sentence claims that "the defense did not even have any information indicating the size of the VM." (Mot. 81).

- Schulte asserts that the virtual machine on his workstation "contained numerous other transcript files—files that he purposefully recorded while performing system administration." (Mot. 82). As discussed above, Schulte's assertions about "transcript files" are false; he refers to data from deleted space. But in discovery Schulte was given log files and data from unallocated space on his VM, and records from the unallocated space were introduced at trial. (D.E. 329 at 8; GX1703-1 at 6, 20, 36, 38, 46, 47, 55, 69, 71, 75, 76, 78-81, 83, 86, 88-90; GX1203-1, -5, -6. -8. -18, -19, -29, -31, -32, -36, -42, -44, -53, -55, -56, -57, -58, -60).

- Schulte asserts that "there was a history of corrupt log files [on the OSB ESXi server] and deleting them," but "none of this could come out at trial." (Mot. 83). Log files from the OSB ESXi server were produced to Schulte in forensic and native format, permitting him to explore his corrupted-log-file theory. (D.E. 329 at 8, D.E. 423 at 2).

- Schulte asserts that he "executed the mount command for the altabackups countless times in his virtual machine and on the other virtual servers from the ESXi Server" but, "without access to a forensic image of the ESXi Server or Mr. Schulte's own Workstation, the defense could not cross-examine Mr. Leedom or present any defense." (Mot. 84; id. 93-94 (any "Confluence regular user could access the altabackup mount.")). Schulte told the FBI in March 2017, however, that he accessed the Altabackup directory from the Stash server (which required a mount point to write the backup files), not from any other location. (Tr. 233). Mr. Weber similarly testified that he accessed the Altabackup directory from the Confluence virtual server. (Tr. 1600). In any event, Schulte was provided in discovery with log files from the three hard drives and virtual machine that made up his CIA workstation and log files and unallocated space from the OSB ESXi server. (D.E. 329 at 8). Some of these records were introduced at trial, showing Schulte's failed attempt to mount a datastore to the Altabackup directory. (GX1703-1 at 12-13, GX1202-7, GX1202-8; Tr. 813-15). Schulte also had the opportunity to cross-examine Mr. Weber, another former Atlassian administrator, about these matters.

- Schulte contends that he "regularly logged into the ESXi Server with his SSH key and kept his sessions open," but could not cross examine Mr. Leedom "without access to the ESXi server." (Mot. 85-86). Schulte was provided in discovery with OSB ESXi server logs (D.E. 329 at 8, D.E. 423 at 2) and records from the auth.log file, which records server logins, was introduced at trial. (GX1703-1 at 15, 19, 26, 33, 45; GX1209-13). Those records do not support Schulte's assertion, but they were available for his use during cross-examination and as admitted evidence.

- Schulte argues he needed access to the entire Confluence and Stash servers to "check the backup script." (Mot. 91). The backup script was produced in discovery and introduced at trial, and Schulte had the opportunity to cross-examine witnesses about it. (GX1207-17; Tr. 768-70).

- Schulte also argues that he needed access to source code for CIA cyber tools to show "it would not be possible to identify the tools based solely on Mr. Schulte's generic statements in his private notebooks." (Mot. 96). Schulte was not charged with

> disclosing source code that was NDI; he was charged with attempting to disclose that a publicly identified malware was a CIA cyber tool, which has nothing to do with the underlying source code.

In sum, Schulte's request for a new trial based on his requests for "unfettered access" to the DevLAN network (D.E. 823 at 3 (quoting D.E. 124)) should be denied.

2. AFD Discovery

As described above, Schulte sought to compel the production of a non-existent AFD report prior to trial. That request was properly denied, and provides no basis for a new trial.

3. Alleged Prosecutorial Misconduct

Schulte's Motion does not identify any prosecutorial misconduct. The referenced statements in jury addresses are all soundly based on trial evidence and the Court's jury instructions. During his closing statement, Schulte in fact acknowledged that he executed the commands reflected in GX1703-1, including the deletion of log files; and, indeed, Schulte claimed that he intentionally made a record of those actions. (Tr. 2209-14). The trial testimony showed that the Altabackup directory could only be accessed from the Atlassian product servers, like the Confluence virtual server and the Stash server, and that Atlassian administrator privileges were needed to log in to the servers. Mr. Leedom testified extensively how the error in the backup script showed that the March 3, 2016, Confluence backups were the source of the WikiLeaks disclosure. Schulte complains that the Government claimed his desk was near the bathroom ("the door is like steps from his desk" (Tr. 2276)), but the floorplan shows that no part of the vault was more than a short walk to the door. (GX111). Finally, reminders that that Schulte's statements were not evidence reflect the Court's instructions. (*E.g.*, Tr. 2252, 2269, 2306). Schulte has not shown any prosecutorial misconduct whatsoever.

CONCLUSION

For the foregoing reasons, the Government respectfully submits that the Court should deny Schulte's Rule 29 and Rule 33 motions.

Dated: New York, New York
March 16, 2023

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

By: /s/
David W. Denton, Jr. / Michael D. Lockard
Assistant United States Attorneys
(212) 637-2744/-2193

Cc: Joshua Adam Schulte (by U.S. Mail)
Defense counsel (by ECF)